KATZ, KYLLO, AND TECHNOLOGY: VIRTUAL FOURTH AMENDMENT PROTECTION IN THE TWENTY-FIRST CENTURY

Tracey Maclin[*]

INTRODUCTION

The freedoms established in the Bill of Rights—including the Fourth Amendment right to be free from unreasonable governmental searches and seizures—were meant to endure. Advances in science and technology recurrently exert pressure on the scope and meaning of the Fourth Amendment,[1] but the privacy and security protected by the Fourth Amendment should not depend on innovations in technology. "When the American Republic was founded, the framers established a libertarian equilibrium among the competing values of privacy, disclosure, and surveillance. This balance was based on the technological realities of eighteenth-century life."[2] During

[*] Professor of Law, Boston University School of Law. I want to thank Tom Clancy for inviting me to speak at the University of Mississippi School of Law and to attend a symposium entitled, The Effect of Technology on Fourth Amendment Analysis and Individual Rights. I also want to thank the National Center for Justice and the Rule of Law at the University of Mississippi School of Law that is supported by a grant from the Bureau of Justice Assistance, Office of Justice Programs, of the U.S. Department of Justice, for its generous support of this article. Finally, I thank Jill Marr for her research assistance.

[1] As Justice Scalia notes: "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." Kyllo v. United States, 533 U.S. 27, 33-34 (2001); *see also* Raymond Shin Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1344 (2002) (arguing that "[f]rom the beginning, the Supreme Court has taken a narrow view of the Fourth Amendment's role in limiting government discretion to employ novel technologies"); Thomas K. Clancy, *What Does The Fourth Amendment Protect: Property, Privacy, or Security*, 33 WAKE FOREST L. REV. 307, 335 (1998) (noting that the "overall tendency of the Court has been to contract the protected individual interest as a consequence of modern technological advances and their utilization by the government").

[2] ALAN F. WESTIN, PRIVACY AND FREEDOM 67 (1967).

the Framers' era, the home was the focal point of privacy and personal security.[3] The Fourth Amendment proscribed intrusions into a home unless a government official obtained a judicial warrant supported by specific procedural safeguards.[4]

With the increased use of technology in the twentieth century, the Supreme Court confronted search and seizure questions never imagined by the Framers. During the first-half of the twentieth century, Fourth Amendment liberties typically fared poorly under the pressure of a technologically advancing society. For example, police investigative methods adapted to deal with the mobility of cars when automobile travel became accessible to many people. In 1925, the Court ruled a warrantless search of a car and its contents is reasonable, provided there is probable cause to believe that the vehicle contains contraband.[5] Three years later, the Court ruled the Fourth Amendment did not encompass police wiretapping of telephone conversations. The Court explained wiretapping involves neither a search nor seizure within the meaning of the Amendment,[6] and that "one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the [Fourth] Amendment."[7] By the 1950's, pressure mounted, on and off the Court, to reconsider whether the Amendment's protective scope excluded wiretapping. Notwithstanding the criticism of its wiretapping ruling, in 1952 the Court held that use of a "wired spy" to capture the conversations of the defendant and a government informant who surreptitiously recorded them did not trigger Fourth Amendment protection.[8] The Court, however, scoffed at the notion that police use of a wired informant is akin to police

[3] *See, e.g.*, DAVID H. FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND 45 (1967).

[4] *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 551 (1999) ("The historical statements about search and seizure focused on condemning general warrants. In fact, the historical concerns were almost exclusively about the need to ban house searches under general warrants.").

[5] Carroll v. United States, 267 U.S. 132, 149 (1925).

[6] Olmstead v. United States, 277 U.S. 438, 464 (1928). *Olmstead* explained that the Fourth Amendment does not forbid wiretapping. "There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants." *Olmstead*, 277 U.S. at 464.

[7] *Id.* at 466.

[8] On Lee v. United States, 343 U.S. 747, 751 (1952).

wiretapping.[9]

Although the Court gave the police wide discretion to utilize technology to investigate individuals during the first half of the twentieth century,[10] the Court transformed its analytical approach toward electronic surveillance in the mid-1960's. First, the Court rejected its earlier conclusion that oral communications were not covered by the Fourth Amendment.[11] The Court then decided three cases which demonstrated a dramatic shift in the Justices' thoughts about electronic surveillance methods. Having previously determined that law enforcement officials could freely use wiretapping and wired informants without constitutional restraint, by 1967 the Court reversed course and ruled that judicial approval was a pre-condition to validate electronic surveillance.

In the first case, *Osborn v. United States*,[12] the Court approved a judicial order authorizing a tape recording of an attorney's conversation with a government informant. A detailed affidavit alleged that the attorney attempted to bribe a juror.[13] The *Osborn* Court specifically noted that the challenged electronic surveillance involved police

[9] *On Lee*, 343 U.S. at 754. The *On Lee* Court asserted: "It would be a dubious service to the genuine liberties protected by the Fourth Amendment to make them bedfellows with spurious liberties improvised by farfetched analogies which would liken eavesdropping on a conversation, with the connivance of one of the parties, to an unreasonable search or seizure." *Id.*

[10] In cases where electronic surveillance constituted a physical trespass or entry into a constitutionally protected area, Fourth Amendment safeguards were imposed. *Compare* Silverman v. United States, 365 U.S. 505, 510-12 (1961) (use of a "spike mike"–which is a device that made contact with a heating duct serving the house occupied by the defendants–was "an unauthorized physical penetration" of the premises, and thus a search under the Fourth Amendment), *with* Goldman v. United States, 316 U.S. 129, 135 (1942) (use of a detectaphone—which captures sound waves–placed against the wall of an office in order to overhear conversations in an adjoining office was no search because there was no physical trespass of the targeted office).

[11] *Olmstead* concluded that oral communications were not protected by the Fourth Amendment. *Olmstead*, 277 U.S. at 464. This conclusion was later rejected in *Silverman*, 365 U.S. at 511 (finding a Fourth Amendment violation because "the officers overheard the petitioners' conversations only by usurping part of the petitioners' house or office" without judicial authorization) and *Wong Sun v. United States*, 371 U.S. 471, 485 (1963) (explaining that *Silverman* recognizes that "the Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of `papers and effects.'"). *Cf.* United States v. White, 401 U.S. 745, 775 (1971) (Harlan, J., dissenting) (noting that *Wong Sun* "expressly brought verbal communications within the sweep of the Fourth Amendment").

[12] 385 U.S. 323 (1966).

[13] *Osborn*, 385 U.S. at 328.

monitoring "under the most precise and discriminate circumstances."[14] *Osborn* was an unusual case because government agents had sought judicial approval *before* undertaking electronic monitoring. Thus, *Osborn* was an unlikely precedent to affect major change in the way law enforcement officials conducted electronic surveillance. The discerning reader, however, would recognize that *Osborn* signaled the Justices' discomfort with previous rulings upholding electronic surveillance.[15]

While *Osborn* may not have caught the attention of law enforcement officials, a second case, *Berger v. New York*,[16] was a bombshell for the police. *Berger* invalidated New York's electronic surveillance statute. The Court found that the electronic surveillance that the statute authorized contained numerous constitutional flaws.[17] Beyond the specific constitutional objections that the majority listed, some of the *Berger* Court's harsh language condemning the New York statute "left the dissenting Justices (and many others) wondering whether *any* wiretapping or electronic

[14] *Id.* at 329.

[15] Prior to *Osborn*, in *Lopez v. United States*, 373 U.S. 427 (1963), the Court upheld the admission of testimony of an Internal Revenue agent's conversation with a defendant who had tried to bribe the agent and a tape recording of that conversation that was captured by a pocket recorder worn by the agent. *Lopez*, 373 U.S. at 440. The *Lopez* Court ruled that no unconstitutional invasion of Lopez's office occurred because the agent had the defendant's "consent, and while there [the agent] did not violate the privacy of the office by seizing something surreptitiously without petitioner's knowledge." *Id.* at 438. Four members of the *Lopez* Court wanted to overrule *On Lee. See id.* at 441-43 (Warren, C.J., concurring) (arguing that *On Lee* should be overruled, but distinguishing facts in *Lopez* from *On Lee* because the use and purpose of the electronic recording equipment in *On Lee* "was not to corroborate the testimony of the [government informant], but rather, to obviate the need to put him on the stand"); *see id.* at 446-53 (Brennan, J., dissenting) (arguing that *On Lee* and *Lopez* are indistinguishable). The *Osborn* majority avoided the debate that was left unsettled in *Lopez* "because it is evident that the circumstances under which the tape recording was obtained in this case fall within the narrower compass of the *Lopez* concurring and dissenting opinions." *Osborn*, 385 U.S. at 327.

[16] 388 U.S. 41 (1967).

[17] *Berger*, 388 U.S. at 56, 58-59. *Berger* explained that the statute was unconstitutional because first, "[i]t lays down no requirement for particularity in the warrant as to what specific crime has been or is being committed, nor `the place to be searched,' or `the persons or things to be seized' as specifically required by the Fourth Amendment." *Id.* at 56; *see also id.* at 58-59. Second, the statute authorized surveillance "for a two-month period [which] is the equivalent of a series of intrusions, searches and seizures pursuant to a single showing of probable cause" and permitted extensions of surveillance on "a mere showing that such extension is `in the public interest.'" *Id.* at 59. Third, the statute "places no termination date on the eavesdrop once the conversation sought is seized. This is left entirely in the discretion of the officer." *Id.* at 59-60. Finally, the statute did not require prompt return on the warrant "thereby leaving full discretion in the officer as to the use of seized conversations of innocent as well as guilty parties." *Id.* at 60.

eavesdropping statute could pass constitutional muster."[18]

Finally, *Katz v. United States*,[19] decided a year after *Osborn*, eliminated any lingering uncertainty about the constitutional validity of unchecked police wiretapping. *Katz* held that FBI agents violated the Fourth Amendment when, without judicial authorization, they attached an electronic listening and recording device to the outside of a public telephone booth that the defendant used.[20] *Katz* was a landmark case.[21] The ruling not only solidified the Court's view that the Constitution required judicial supervision of electronic surveillance, it also "purported to clean house on outmoded [F]ourth [A]mendment principles."[22] Moreover, in the view of many, the impact of *Katz* was "to expand rather than generally to reconstruct the boundaries of [F]ourth [A]mendment protection."[23] Put simply, the holding and logic of *Katz* was revolutionary. *Katz* moved the Court "toward a redefinition of the scope of the [F]ourth [A]mendment."[24] The passage of time, however, would show that *Katz* would do little to protect Fourth Amendment liberties.

The technological advances of the twenty-first century will present new, and sometimes more challenging, issues as judges grapple with the question of how much privacy and security the Fourth Amendment provides.[25] At the start of

---

[18] YALE KAMISAR ET AL., BASIC CRIMINAL PROCEDURE: CASES, COMMENTS AND QUESTIONS 352-53 (10th ed. 2002).

[19] 389 U.S. 347 (1967).

[20] *Katz*, 389 U.S. at 359.

[21] *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.1(b), at 385 (3d ed. 1996).

[22] Note, *From Private Places to Personal Privacy: A Post-*Katz *Study of Fourth Amendment Protection*, 43 N.Y.U. L. REV. 968, 975 (1968).

[23] Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 385 (1974).

[24] Edmund W. Kitch, Katz v. United States: *The Limits of the Fourth Amendment*, 1968 SUP. CT. REV. 133, 133; *see also* Stephen A. Saltzburg, *Another Victim of Illegal Narcotics: The Fourth Amendment (As Illustrated by the Open Fields Doctrine)* 48 PITT. L. REV. 1, 11-12 (1986) (explaining how *Katz* tends to redefine the scope of the Fourth Amendment); Albert W. Alschuler, *Interpersonal Privacy and the Fourth Amendment*, 4 N. ILL. U. L. REV. 1, 6 n.12 (1983) (explaining how *Katz* ties the right to privacy to "changing cultural expectations" of privacy). *Cf.* David A. Sklansky, *Back To The Future*: Kyllo, Katz, *and Common Law*, 72 MISS. L.J. 143, 145 (2002) (describing *Katz* as "perhaps the most influential search-and-seizure decision of the past half-century").

[25] *Cf.* Susan Bandes, *Power, Privacy and Thermal Imaging*, 86 MINN. L. REV. 1379, 1383 (2002) ("On a more basic level, technology advances pose the challenges that always beset the constitutional enterprise–those involved with trying to create fixed rules, or at least a workable rule of law, for a changing world. In this regard, technology *illustrates* the problem with trying to rely on

this new century, the Court decided *Kyllo v. United States*,[26] which in tone and substance resembles *Katz*. *Kyllo* ruled that a thermal imaging device directed at a home constituted a search within the meaning of the Fourth Amendment.[27] The Court explained that a search occurs when government agents use sense-enhancing technology to collect any information regarding the interior of a home that could not otherwise be obtained without a physical invasion, "at least where (as here) the technology in question is not in general public use."[28] Like *Katz*, *Kyllo* is an important case for assessing the Court's current thinking on the interplay of technology and the Fourth Amendment. *Kyllo*'s long-term

fixed understandings of how the world works."); Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. & TECH. L. REV. 61, 70 (2000) (noting the danger "that courts will rigidly adhere to outdated Fourth Amendment concepts which are ill-suited to cyberspace, leading to the conclusion that Web users lack legitimate expectations of privacy in clickstream data"). Occasionally, the key to resolving an emerging issue of the twenty-first century requires application of traditional constitutional doctrine. For example, Professor Orin Kerr has noted that "[a]lthough the Internet is a recent development with great promise for revolutionary change, the Fourth Amendment questions raised by encrypting Internet communications are decades (if not centuries) old." Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"* 33 CONN. L. REV. 503, 532 (2001). In an insightful article, Professor Kerr contends that encryption cannot create a constitutionally protected privacy interest, and government efforts to unscramble an encrypted communication do not constitute searches under the Fourth Amendment. *Id*. at 517-24. Professor Kerr predicts that in resolving this issue, judges will ultimately discover that the Fourth Amendment issue raised by encryption "involve[s] old wine in new bottles." *Id*. at 532.

[26] 533 U.S. 27 (2001).

[27] *Kyllo*, 533 U.S. at 40.

[28] *Id*. at 34. *Kyllo*'s holding is announced in two different places in Justice Scalia's opinion. *See id*. ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical `intrusion into a constitutionally protected area' constitutes a search–at least where (as here) the technology in question is not in general public use.") (citation omitted); *id*. at 40 ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a `search.'"). As Professor Christopher Slobogin perceptively explains, although *Kyllo*'s holding *expands* Fourth Amendment protection to include thermal imaging, it also *shrinks* the constitutional protection afforded private homes by codifying a "naked eye" exception to the warrant requirement. *See* Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo's *Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1410 (2002) (explaining that, taken together, *Kyllo*'s holdings "announce that if the activity observed could be seen with the naked eye without physical intrusion into the constitutionally protected areas of home or curtilage, then police may exploit *any* technology–generally used or not–without implicating the Fourth Amendment."); *id*. at 1414 (noting that *Kyllo* "holds that enhanced searches of the home are permissible if they merely duplicate naked eye searches from vantage points that are not constitutionally protected").

impact on search and seizure doctrine, however, remains uncertain.

In a thoughtful and well-reasoned article, Professor David Sklansky states that *Kyllo* is likely to be one of the "touchstones" for the Court when it decides future cases involving the government's ability to use technology to gather information and fight terrorism.[29] According to Professor Sklansky, "[e]ven before [the] September 11 [terrorist attacks] . . . , it was apparent that *Kyllo* had significance beyond its narrow holding and beyond its value as a curiosity."[30] While I agree with much of Professor Sklansky's analysis of *Kyllo*, I do not share his view that *Kyllo*'s analytical framework will be a "touchstone[]" for future disputes involving technology and the Fourth Amendment. I predict that *Kyllo*'s impact on protecting Fourth Amendment liberties, like *Katz*, will be slight. Just as the Court later confined the "right" established in *Katz* to a privilege against clandestine wiretapping and electronic bugging without judicial supervision,[31] the Court is likely to construe the "right" announced in *Kyllo* narrowly. In other words, *Kyllo*, like *Katz*, will not prevent police officials from using other types of technology to monitor and discover information helpful to law enforcement interests.

Part I of this article briefly discusses the similarities between *Katz* and *Kyllo*. This section describes the common traits shared by *Katz* and *Kyllo*: both cases were immediately recognized as important rulings, both cases signaled a shift or readjustment of Fourth Amendment law, and both cases rest on a simple, but persuasive logic about the scope of protection provided by the Fourth Amendment. Part II analyzes the substance of the *Katz* ruling and considers the long-term impact of *Katz* for protecting Fourth Amendment rights against technological innovations. This section contends that *Katz* has failed to protect Fourth Amendment rights for two reasons. First, *Katz* was a ruling without substance. Second, the Justices who decided *Katz* were unable to agree on the meaning of their ruling, which made it easier for future Justices to ignore the relevance of *Katz* in subsequent cases concerning the reach of the Fourth

[29] Sklansky, *supra* note 24, at 144.
[30] Sklansky, *supra* note 24, at 145.
[31] *See, e.g.*, United States v. United States Dist. Ct., 407 U.S. 297, 308 (1972).

Amendment.

Part III considers what impact *Kyllo* may have on future cases involving technology and the Fourth Amendment. Although *Kyllo*'s impact on Fourth Amendment liberties is uncertain at this point, this section argues that *Kyllo* is unlikely to prevent government officers from using technology to monitor and reveal information. The final section of the article, Part IV, examines how the Court might address the constitutional status of e-mail addressing information and whether Carnivore's pen mode intercept constitutes a search under the Fourth Amendment in a post-*Kyllo* world. Part IV contends that if Carnivore's pen mode intercept is judged by the rule announced in *Kyllo*, then the Court should find that this intrusion is a search. Nevertheless, Part IV concludes with the prediction that the Court will find that Carnivore's pen mode intercept does not violate the Fourth Amendment.

I. THE SIMILARITIES BETWEEN *KATZ* AND *KYLLO*

A. Both cases were immediately recognized as significant rulings

Katz and *Kyllo* share three prominent characteristics. First, the public and legal profession recognized both cases as significant rulings that would impact Fourth Amendment doctrine. Legal commentators and the press immediately recognized *Katz* as an important case. The press commented on the break from the trespass rule[32] and expressed surprise that the Court was willing to uphold *any* electronic surveillance,[33] while legal commentators commented on the Court's new methodology for determining when a search occurs.[34] Likewise, while *Kyllo* involved rather narrow facts,

[32] Fred P. Graham, *A Plug in the `Big Ear,'* N.Y. TIMES, Dec. 24, 1967, § 4, at 10 ("Last week the Supreme Court faced up to the scientific facts of life and held that the Fourth Amendment covers all police eavesdropping, whether accomplished by means of a trespass into private premises or not.").

[33] *See id.* ("[That the Court added that the bugging in *Katz* would have been constitutional had a search warrant been procured] caught many lawyers by surprise, because the tone of the Supreme Court's recent eavesdrop decisions has been so hostile that people assumed the Justices would hedge police-bugging in with so many legal technicalities that almost any useful eavesdropping would be deemed unconstitutional."); Fred P. Graham, N.Y. TIMES, Dec. 19, 1967, at A1 ("[T]he wording of the [*Katz*] decision erased an impression that had been created in a decision of the Court last June that the Supreme Court would insist on such elaborate procedures in connection with these warrants that bugging would become virtually useless as a police tool.").

[34] *See, e.g.*, Note, *From Private Places to Personal Privacy: A Post-*Katz *Study of Fourth Amendment Protection*, 43 N.Y.U. L. REV. 968 (1968)

the press and legal academics quickly noted the significance of the ruling and the possible effect the ruling could have on the government's use of technology.[35]

B. Both cases readjusted Fourth Amendment law

Both *Katz* and *Kyllo* also signaled a shift, or readjustment, in Fourth Amendment law. *Katz*, authored by Justice Stewart, explicitly rejected two concepts that previously influenced the shape of search and seizure

(describing *Katz* as a "landmark" case); *id.* at 981 ("[T]he *Katz* decision has pointed the way towards a complete re-orientation in the analysis of problems relating to governmental intrusion into individuals' private affairs."); *id.* ("Rather than relying on an interpretation of the nature and legitimacy of the Government's searching activity, the Court's holding was based solely on the validity of the individual's expectation of privacy. . ."); Kitch, *supra* note 22, at 133 ("The Supreme Court is moving toward a redefinition of the scope of the Fourth Amendment. *Katz v. United States*, . . . indicates that the Court is now prepared to release the Fourth Amendment, . . . from the moorings of precedent and determine its scope by the logic of its central concepts.") (footnotes omitted).

[35] *See, e.g.*, Linda Greenhouse, *The Supreme Court: Ruling on Surveillance Procedures; Justices Say Warrant Is Required in High-Tech Searches of Homes*, N.Y. TIMES, June 12, 2001, at A1 (describing *Kyllo* as an "important declaration of the constitutional limits on new privacy-threatening technology"); Linda Greenhouse, *As Crime Ebbs, Top Court's Privacy Rulings Flow*, N.Y. TIMES, June 17, 2001, § 4, at 16 (noting: "It is almost as if the public, liberated from the burdensome presence of crime, is free to express doubts about the civic costs of a whole range of crime-fighting strategies, from racial profiling to high-tech eavesdropping to low-tech drug-sniffing dogs."); David G. Savage, *Court Says No to Home Snooping Law: U.S. Justices Restrict the Use of Heat Sensors and Other High-Tech Spy Devices by Police*, L.A. TIMES, June 12, 2001, at A1 ("The ruling appears to put a significant limit on the government's use of new technologies that can pick up sounds or images inside a home . . . . The decision itself marked the third major ruling this year in which the justices have rejected drug searches and put new limits on the war on drugs."); Edward Walsh, High-Tech Devices Require a Warrant; Court: Search Violates Privacy Right, WASH. POST, June 12, 2001, at A1 ("`It means that the Fourth Amendment is going to apply to all the high-tech technology that is rapidly being developed. Big Brother must now pay attention to constitutional principles.'") (quoting Steven R. Shapiro, national legal director of the American Civil Liberties Union); *cf. id.* ("`It is an additional step they have to go through. The Fourth Amendment is important, privacy is important, but this is not a blockbuster case.'") (quoting Kent Scheidegger, legal director of Criminal Justice Legal Foundation); Michelle M. Jochner, *Privacy Versus Cyber-Age Police Investigation: The Fourth Amendment in Flux*, 90 ILL. BAR J. 70 (describing *Kyllo* as a "landmark decision"); *id.* ("The Court's decision in *Kyllo* makes it clear that although technology have evolved, the intent underpinning the Fourth Amendment remains constant."). Two other commentaries have discussed *Kyllo*. *See* Sean D. Thueson, *Fuzzy Shades of Gray: The New "Bright-Line" Rule in Determining When the Use of Technology Constitutes a Search*, 2 WYO. L. REV. 169 (2002); Sarilyn E. Hardee, *Why the United States Supreme Court's Ruling in* Kyllo v. United States *Is Not the Final Word on the Constitutionality of Thermal Imaging*, 24 CAMPBELL L. REV. 53 (2001).

doctrine. Prior to *Katz*, a judicial finding that the challenged police action invaded a "constitutionally protected area" was necessary to trigger the Amendment's safeguards.[36] In their briefs to the Court, the litigants contested whether a public telephone booth was a constitutionally protected area. Justice Stewart, however, found the debate unhelpful. "[T]his effort to decide whether or not a given `area,' viewed in the abstract, is `constitutionally protected' deflects attention from the problem presented by this case."[37] At this point, Justice Stewart wrote the lines that would symbolize the meaning and spirit of *Katz*:

> For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[38]

In addition to dismissing the importance of whether the intrusion compromised a constitutionally protected area, *Katz* also rejected the rule that invocation of Fourth Amendment protection required a physical intrusion or "trespass" by government officials.[39] Justice Stewart acknowledged that the Court's previous rulings barred constitutional scrutiny of police intrusions in the absence of a physical penetration because the Amendment "was thought to limit only searches and seizures of tangible property."[40] Justice Stewart, however, explained that the "trespass" rule was no longer viable in light of the Court's more recent rulings that the Amendment covers the seizure of oral statements, even when a police intrusion was not a trespass under local property law. "Once this much is acknowledged, and once it is recognized that the Fourth Amendment protects people—and not simply `areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any

---

[36] *See* 1 LAFAVE, *supra* note 21, § 2.1(a) at 380 (explaining that what the pre-*Katz* cases "added up to, as the Supreme Court was later to put it, was that for there to be a Fourth Amendment search the police must have physically intruded into `a constitutionally protected area'") (citations and footnote omitted). In *Katz*, Justice Stewart acknowledged this point, although he sought to downplay the determinative weight given in prior cases to the concept of a "constitutionally protected area." *See* Katz v. United States, 389 U.S. 347, 351, n.9 (1967) (explaining that the Court has "never suggested that this concept can serve as a talismanic solution to every Fourth Amendment problem.").

[37] *Katz*, 389 U.S. at 351 (footnote omitted).

[38] *Id* at 351-52 (citations omitted).

[39] *Id.*

[40] *Id.* at 352-53 (footnote omitted).

given enclosure."[41] Thus, with bold strokes, *Katz* rejected previous understandings that had dictated the reach and meaning of the Fourth Amendment. After *Katz*, the scope of the Amendment would not only be loosened from the ancient niceties of common-law property rules, but the substantive content of the Amendment would derive from thoroughly modern and realistic understandings of the privilege against unreasonable searches and seizures.[42]

Like *Katz*, *Kyllo* also represents a shift, albeit subtle, in the Court's approach to defining what is a "search" under the Amendment. The government contended that the thermal imaging directed at Kyllo's home was not a search because it did not reveal any intimate details of his home.[43] The Court's "threshold" cases seemed to support the Government's position. Indeed, since at least 1984, the Court had strongly intimated that police intrusions directed at homes might not trigger constitutional inquiry unless those intrusions interfered with or revealed intimate activities associated with the home. For example, in *Oliver v. United States*,[44] the Court explained that the Amendment's protection of "houses" went beyond merely protecting the physical interior of a home; it also protected the curtilage of the home.[45] Citing the common law, *Oliver* opined that the curtilage "is the area to which extends the intimate activity associated with the `sanctity of a man's home and the privacies of life,' and therefore has been

[41] *Id*. at 353.

[42] *See id*. at 352 ("No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communications."). Professor Amsterdam cogently recognized that the crucial question at stake in a case like *Katz* is "a value judgement." Amsterdam, *supra* note 23 at 403 ("The ultimate question, plainly, is a value judgment. It is whether, if the particular form of surveillance practiced by the police is permitted to go unregulated by constitutional restraints, the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with aims of a free and open society.").

[43] *See* Brief for the United States at 22, *Kyllo* (99-8508) ("This Court's decisions establish . . . that the Fourth Amendment does not preclude the government from obtaining the assistance of technology to observe an area that is exposed to the public, provided that the technology does not permit the government to detect *private* activities occurring in the private areas.") (emphasis added).

[44] 466 U.S. 170 (1984).

[45] *Oliver*, 466 U.S. at 181 n.12.

considered part of the home itself for Fourth Amendment purposes."[46]

United States v. Dunn[47] elevated *Oliver*'s dicta on the meaning of curtilage to law. In *Dunn*, the Court adopted *Oliver*'s definition of curtilage and noted that a "central component of th[e] inquiry [regarding the extent of a home's curtilage is] whether the area harbors the intimate activity associated with the `sanctity of a man's home and the privacies of life.'"[48] *Dunn* then identified several factors for determining whether a particular area fell within the curtilage of a home.[49] One factor considered "the nature of the uses to which the area is put."[50] When applying this criterion to the facts in *Dunn*, the Court explained that it was "especially significant that the law enforcement officials possessed objective data indicating that the [area] was not being used for intimate activities of the home."[51]

Oliver and *Dunn* were not the only cases lending support to the government's claim in *Kyllo* that police conduct directed at a home did not trigger constitutional scrutiny unless it revealed intimate details of the home. The Court held in *California v. Ciraolo*[52] that no search occurred when police officers, flying in navigable airspace, observed marijuana growing in a fenced-in backyard.[53] The fact that the activities that the police observed lay within the curtilage did not help Ciraolo.[54] The Court ruled that the flyover was not a search because the surveillance occurred in "a physically nonintrusive manner" and within "public navigable airspace."[55] Although *Ciraolo* ruled that police flyovers do not trigger Fourth Amendment review, the Court left open the possibility that other types of aerial observations might produce a different result.[56] In particular, the Court highlighted the State's concession that "`[a]erial observation of curtilage may become invasive, either due to physical

---

[46] *Id.* at 180 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

[47] 480 U.S. 294 (1987).

[48] *Dunn*, 480 U.S. at 300 (quoting *Oliver*, 466 U.S. at 180) (internal quotation marks omitted).

[49] *Id.* at 301.

[50] *Id.* The Court also looked to "the proximity of the area claimed to be curtilage to the home, whether the area is included within an inclosure surrounding the home . . . and the steps taken by the resident to protect the area from observation by people passing by." *Id.*

[51] *Id.* at 302.

[52] 476 U.S. 207 (1986).

[53] *Ciraolo*, 476 U.S. at 215.

[54] In *Oliver* and *Dunn*, the police intrusions did not breach the curtilage.

[55] *Ciraolo*, 476 U.S. at 213.

[56] *Id.* at 215.

intrusiveness or through modern technology which discloses to the senses those *intimate* associations, objects or activities otherwise imperceptible to police or fellow citizens.'"[57]

Three years after deciding *Ciraolo*, in *Florida v. Riley*[58] the Court ruled that helicopter surveillance of a greenhouse adjacent to a home was not a search.[59] Noting that *Ciraolo* controlled this case, Justice White's plurality opinion explained that "because the sides and roof of his greenhouse were left partially open" and because the observation occurred while the helicopter was in navigable airspace, Riley could not reasonably have expected that the interior of the greenhouse would remain free from police inspection.[60] At the end of his opinion, however, Justice White acknowledged that the helicopter observation did not interfere with the normal use of the greenhouse or other parts of the curtilage and, most importantly, "no intimate details connected with the use of the home or curtilage were observed."[61]

Relying on these cases and others not involving intrusions of homes, the government argued in *Kyllo* that thermal imaging was not a search because it did not "`detect private activities occurring in private areas.'"[62] This argument, however, did not persuade Justice Scalia. According to Scalia, "[t]he Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."[63] Justice Scalia then stated: "In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."[64]

---

[57] *Id.* at 215, n. 3, quoting Brief for Petitioner 14-15 (emphasis added). In *Dow Chem. Co. v. United States*, 476 U.S. 227 (1986), the Court held that aerial photography of an industrial complex did not constitute a search. *Dow Chem. Co.*, 476 U.S. at 234. While acknowledging that the use of "highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, *might* be constitutionally proscribed absent a warrant," the Court stressed that the challenged photos did not reveal "intimate details as to raise constitutional concerns." *Id.* at 238 (emphasis added).

[58] 488 U.S. 445 (1989).

[59] *Riley*, 488 U.S. at 448.

[60] *Id.* at 448-50.

[61] *Id.* at 452.

[62] Kyllo v. United States, 533 U.S. 27, 37 (2001) (quoting Brief for United States at 22); *see also* Andrew Riggs Dunlap, *Fixing the Fourth Amendment with Trade Secret Law: A Response to* Kyllo v. United States, 90 GEO. L.J. 2175, 2184-85 (2002) (noting cases where the Court suggested that unless government conduct revealed "intimate details" of the home, no search occurred).

[63] *Kyllo*, 533 U.S. at 37.

[64] *Id.*

Thus, the information that the thermal imaging device revealed, "how warm—or even how relatively warm—Kyllo was heating his residence," was protected against government snooping.[65]

Therefore, with little fanfare, *Kyllo* turned aside a momentum that had been building in the Court's prior cases.[66] Those cases suggested that unless the challenged police conduct compromised intimate activities of the home, Fourth Amendment review was unavailable.[67] Justice Scalia's opinion signals a readjustment in the Court's thinking on this issue.[68] Just as *Katz* discarded a narrow view of the Fourth Amendment's scope,[69] *Kyllo* also rejected the notion that a

[65] *Id.* at 38 (footnote omitted). Justice Scalia dismissed the government's reliance on *Ciraolo*'s dictum cautioning against police use of modern technology that exposes "intimate associations, objects or activities otherwise imperceptible to police or fellow citizens." *Id.* at n.5 (quoting *Ciraolo*, 476 U.S. at 215 n.3). In Justice Scalia's view, *Ciraolo*'s "focus in this second-hand dictum was not upon intimacy but upon otherwise-imperceptibility, which is precisely the principle we vindicate today." *Id.* at n. 5.

[66] Justice Scalia asserted that "our cases show, *all* details [of a home] are intimate details, because the entire area is held safe from prying government eyes." *Id.* at 37. But *United States v. Karo*, 468 U.S. 705 (1984) and *Arizona v. Hicks*, 480 U.S. 321 (1987), which are cited by Justice Scalia to support his statement, are rather thin columns to support the rule that "*all* details" of a home are constitutionally protected. *Karo* held that monitoring of a beeper constitutes a search when it reveals information regarding the inside of a home that could not have been obtained through visual surveillance. *Karo*, 468 U.S. at 715. Although *Karo*'s holding is consistent with Justice Scalia's statement, before *Kyllo*, the result in *Karo* had never been understood to stand for the proposition that "*all* details" of a home are constitutionally protected. Rather, the result in *Karo* turned on the fact that the beeper device used there helped the government "obtain information that it could not have obtained by observation from outside the curtilage of the house." *Id.* at 715. Similarly, *Hicks* was about limiting the scope of police entries into homes,[66] rather than establishing a rule that "*all* details" of a home are constitutionally protected. *Hicks*, 480 U.S. at 323. The *Hicks* majority, in an opinion by Justice Scalia, first rejected the government's claim that an officer's moving of stereo equipment to reveal its serial number did not constitute a new "search" because it produced no additional invasion of privacy separate from the already lawful presence of the officer, which was justified by an emergency call that a shooting had occurred inside the premises. *Id.* at 325 Justice Scalia explained that "taking action, unrelated to the objectives of the authorized intrusion, which exposed to view concealed portions of the apartment or its contents, did produce a new invasion of respondent's privacy unjustified by the exigent circumstance that validated the entry." *Id.* at 325. He then noted: "A search is a search, even if it happens to disclose nothing but the bottom of a turntable." *Id.* Interestingly, the holdings in *Karo* and *Hicks* did not prevent the Court from finding that the aerial intrusions in *Ciraolo* and *Riley* were not searches despite the fact that the challenged photography revealed details of the curtilage of private homes.

[67] *See supra* notes 51-53, 65-66 and accompanying text.

[68] *See supra* note 66 and accompanying text.

[69] *See* Katz v. United States, 389 U.S. 347, 353 (1967) (noting that while *Olmstead* held that "surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view").

police intrusion "must be rather substantial and must reveal specifically certain intimate details" to invoke Fourth Amendment scrutiny.[70] For this reason, Professor LaFave applauds Justice Scalia's opinion "for foregoing [one of] the various privacy-belittling techniques that have become rather common in efforts to narrow the protections of the *Katz* doctrine."[71]

A second feature of *Kyllo*'s reasoning—the importance of bright-line rules—also indicates a change of direction, albeit a shift that may be temporary, from the Court's most recent case involving the scope of protection afforded private homes. In *Kyllo*, Justice Scalia stated that restricting "the prohibition of thermal imaging to `intimate details' would not only be wrong in principle; it would be impractical in application, failing to provide `a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment.'"[72] He then noted the inability of police officers to predict the amount of detail that a particular thermal imaging device will reveal.[73] Justice Scalia also wondered whether the Court was capable of articulating a Fourth Amendment rule that identifies which activities of the home are "`intimate' and which are not."[74] And even if the Court announced such a rule, "no police officer would be able to know *in advance* whether his through-the-wall surveillance picks up `intimate' details—and thus would be unable to know in advance whether it is constitutional."[75] Accordingly, Justice Scalia concluded that because the Fourth Amendment "draws `a firm line at the entrance to the house,'"[76] police officers are better served if the line is not "only firm but also bright"—which means "clear specification of those methods of surveillance that require a warrant."[77]

---

[70] 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.2, at 77 (3d ed. 1996) (Supp. 2002).

[71] *Id.* at 76.

[72] *Kyllo*, 533 U.S. at 38 (quoting Oliver v. United States, 466 U.S. 170, 181 (1984)).

[73] *See id.* at 38 (noting "there is no necessary connection between the sophistication of the surveillance equipment and the `intimacy' of the details that it observes—which means that one cannot say (and the police cannot be assured) that use of the relatively crude equipment at issue here will always be lawful").

[74] *Id.* at 39.

[75] *Id.*

[76] *Id.* at 40 (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).

[77] *Kyllo*, 533 U.S. at 40.

Kyllo's emphasis on the importance of bright-line rules is a notable change of direction from the reasoning of the Court in *Minnesota v. Carter*.[78] In *Carter*, a police officer, peering through a gap in the closed blinds of an apartment window, observed three individuals bagging cocaine—the female leaseholder of the premises and two men, Carter and Johns.[79] Police eventually arrested the men outside of the apartment and later learned that the men had entered the apartment for the sole purpose of packaging cocaine, had no prior contact with the premises, and that the men were in the apartment for approximately two-and-one-half hours.[80] The issue confronting the Court was whether Carter and Johns had a legitimate expectation of privacy in their host's home.[81]

Chief Justice Rehnquist's plurality opinion neatly summarized the extant doctrine. "[A]n overnight guest in a home may claim the protection of the Fourth Amendment, but one who is merely present with the consent of the householder may not."[82] The facts in *Carter* were "obviously somewhere in between" the *per se* rules that the Court's prior cases established. The Chief Justice concluded that the men could not invoke the Fourth Amendment's protection because of "the purely commercial nature" of their behavior, their "relatively short period of time [spent] on the premises, and the lack of any previous connection" between the men and their host.[83]

Justice Kennedy wrote a separate concurring opinion providing the fifth vote in *Carter*.[84] Interestingly, Justice Kennedy noted that the "[s]ecurity of the home must be guarded by the law in a world where privacy is diminished by enhanced surveillance and sophisticated communication systems."[85] He also expressed his agreement with the dissenting Justices' view that reasonable expectations of the host "are shared, to some extent, by the guest."[86] For Justice Kennedy, this suggested a general rule: "social guests will

[78] 525 U.S. 83 (1998).
[79] *Carter*, 525 U.S. at 85.
[80] *Id.* at 86
[81] *Id.* at 87.
[82] *Id.* at 90.
[83] *Id.* at 91.
[84] *Id.* at 99.
[85] *Id.* at 99 (Kennedy, J., concurring). Despite this professed concern about privacy being "diminished by enhanced surveillance and sophisticated communications systems," Justice Kennedy dissented in *Kyllo. Id.*
[86] *Id.* at 102. At the start of his opinion, Justice Kennedy explained that he joined the Chief Justice's opinion because "its reasoning is consistent with my view that almost all social guests have a legitimate expectation of privacy, and hence protection against unreasonable searches, in their host's home." *Id.* at 99.

have an expectation of privacy in their host's home."[87] That said, however, Justice Kennedy concluded that Carter and Johns could not rely on the Fourth Amendment's protection because they had "nothing more than a fleeting and insubstantial connection" with their host's home.[88] Justice Kennedy saw no reason "to fashion a *per se* rule of home protection, with an automatic right for all in the home to invoke the exclusionary rule, in order to protect homeowners and their guests from unlawful police intrusion."[89]

Although *Kyllo* and *Carter* both addressed the degree of protection the Fourth Amendment provides for individuals located in a home, *Kyllo*'s stress on the importance of bright-line rules to protect the privacy of the home and to provide guidance for police contrasts sharply with the balancing analysis of *Carter*.[90] Doubtlessly unintended, Justice Scalia's predilection for bright-line rules that protect the home is reminiscent of the *per se* rules that the Warren and Burger Courts established. In cases like *Karo v. United States*,[91] *Steagald v. United States*,[92] *Payton v. New York*,[93] *Mincey v. Arizona*,[94] *Vale v. Louisiana*,[95] *Stoner v. California*,[96] and *Chapman v. United States*,[97] bright-line rules were announced to protect the privacy and security of the home.[98] Countervailing law enforcement interests can usually be found to justify a police intrusion of a home, especially when evidence of criminal conduct is discovered.[99] In the past, the Court developed *per se* rules to pre-empt the *ad hoc* arguments frequently used to compromise Fourth

[87] *Id.* at 102.
[88] *Id.* at 102.
[89] *Id.* at 103.
[90] *See supra* notes 82-83 and accompanying text.
[91] 468 U.S. 705 (1984).
[92] 451 U.S. 204 (1981).
[93] 445 U.S. 573 (1980).
[94] 437 U.S. 385 (1978).
[95] 399 U.S. 30 (1970).
[96] 376 U.S. 483 (1964).
[97] 365 U.S. 610 (1961).
[98] Minnesota v. Olson, 495 U.S. 91, 93 (1989), which held that an overnight guest is entitled to rely on the privacy of his host's home, is an example of a bright-line rule protecting homes announced by the Rehnquist Court.
[99] In his dissent in *Kyllo*, Justice Stevens noted the "strong public interest" served by a thermal imager. *See Kyllo*, 533 U.S. at 45 (Stevens, J., dissenting) ("[P]ublic officials should not have to avert their senses or their equipment from detecting emissions in the public domain such as excessive heat, traces of smoke, suspicious odors, odorless gases, airborne particulates, or radioactive emissions, any of which could identify hazards to the community.").

Amendment interests.[100]

Bright-line rules are also meant to provide guidance to the police; balancing models seldom afford such guidance. The reasoning of the Chief Justice and Justice Kennedy in *Carter* illustrate the dangers of balancing. How is an officer to know in advance whether his "Peeping-Tom" observations are directed at a guest or visitor who is entitled to share his host's privacy? Whether a person is entitled to constitutional protection against arbitrary police snooping should not depend on information that is later discovered by the police. Nor should the constitutionality of an officer's snooping turn on the length of a person's visit or whether he stays overnight. "Otherwise, a homeowner's sexual partner would have no expectation of privacy in the home and no standing to object if the police peered through the closed blinds of a bedroom window, unless that sexual partner spent the night."[101] More importantly, the *ad hoc* balancing analysis in *Carter* undermines the security of private homes. The result in *Carter*, as Professor Susan Bandes notes "encourages . . . searches of homes that invade the privacy of homeowners, so long as it is the visitor, not the homeowner, who is caught with contraband."[102] In sum, Justice Scalia's decision in *Kyllo* to adopt a bright-line rule protecting "*all* details" of the home, no matter how insignificant the information, calls to mind an earlier judicial attitude about Fourth Amendment rules that affect the home and is a notable change of direction from the

---

[100] *See, e.g.*, Mincey v. Arizona, 437 U.S. 385, 393 (1978) (noting that the importance of the state's interest in prompt investigation of a murder, but explaining that a similar interest is extant for other serious crimes; "[i]f the warrantless search of a homicide scene is reasonable, why not the warrantless search of the scene of a rape, a robbery, or a burglary? `No consideration relevant to the Fourth Amendment suggests any point of rational limitation' of such a doctrine.") (quoting Chimel v. California, 395 U.S. 752, 766 (1969)).

[101] Tracey Maclin, *What Can Fourth Amendment Doctrine Learn from Vagueness Doctrine?*, 3 U. PA. J. CONST. L. 398, 434-35 (2001) (footnote omitted). Professor LaFave takes a different view of the impact of *Carter*. According to LaFave:

> *Carter* should not be taken to mean, with regard to a social guest, that if something less than an overnight stay will suffice, the stay must be longer than the [two-and-a-half] hour visit in that case. This is because the Court acknowledged that the situation there fell somewhere between that of the *Olson* overnight guest (who had standing) and one who `merely' is lawfully present (without standing by virtue of the repudiation of [Jones v. United States, 362 U.S. 257 (1960)]), and *then* held it to be closer to the latter *only* after factoring in the lesser expectation of privacy that attends `property used for commercial purposes.' There is no reason why a much shorter-term social visitor should be deemed to lack standing.

Id. at 5 LAFAVE, *supra* note 70, § 11.3 at 23.

[102] Bandes, *supra* note 25 at 1381 (footnote omitted).

Court's most recent ruling involving the protection afforded private homes.

C. Both cases rest on simple, but persuasive logic

A final characteristic that *Katz* and *Kyllo* share is that both cases based their conclusions on a simple, but persuasive, logic. In *Katz*, Justice Stewart explained that a person who enters a telephone booth, "shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[103] A contrary view would "ignore the vital role that the public telephone has come to play in private communication."[104] In *Kyllo*, the crucial factor was that the thermal imaging device enabled the government to discover information about the inside of a home that was otherwise unavailable without a physical intrusion.[105] For Justice Scalia, the legal question in *Kyllo* was straightforward: Should the government be free to gather *any* detail concerning the inside of someone's home without complying with the requirements of the Warrant Clause? In answering this inquiry, Justice Scalia saw a direct link between thermal imaging and the intrusions that writs of assistances and general warrants authorized, which prompted the Framers to adopt the Fourth Amendment.[106] When viewed from this perspective, the answer was clearly "no." A contrary view would compromise "that degree of privacy against government that existed when the Fourth Amendment was adopted."[107]

---

[103] Katz v. United States, 389 U.S. 347, 352 (1967); *see also id.* at 361 (Harlan, J., concurring) (same).

[104] *Id.* Professor Lewis Katz nicely summarizes why *Katz* has been viewed as a "seminal" case. "A seminal case should provide a framework for its later application. However, the seminal quality of *Katz* lies in its understanding of what the [F]ourth [A]mendment is about rather than in the clarity of its rule." Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L. J. 549, 562 (1990).

[105] *See supra* note 73 and accompanying text.

[106] Kyllo, 533 U.S. at 40 (noting that although the compromise of Kyllo's privacy was insignificant, that fact is unimportant: "we must take the long view, from the original meaning of the Fourth Amendment forward").

[107] *Id.* at 34.

II. THE LONG-TERM IMPACT OF *KATZ*

The above discussion establishes that *Katz* and *Kyllo* share certain common traits. Whether *Kyllo*'s long-term impact will be similar to the influence of *Katz* is currently unknown. Although *Kyllo*'s influence has yet to be determined, one can still make predictions about its effect on future Fourth Amendment doctrine. However, before considering *Kyllo*'s potency for the future, it may be instructive to recall the influence of *Katz*. The following section demonstrates that *Katz*'s impact on protecting Fourth Amendment liberties, particularly when technological innovations threaten those liberties, has been insignificant because *Katz* itself lacked substance. A lack of substance, however, was not the only factor contributing to *Katz*'s failure to protect Fourth Amendment liberties. The Justices who decided *Katz* could not agree on *Katz*'s meaning. This lack of consensus about a "landmark" case would make it easier for future Justices to dismiss the relevance of *Katz* in subsequent disputes concerning the Amendment's reach. To the extent that *Kyllo* contains similar defects, its capability and strength to protect Fourth Amendment interests against technological advances may prove to be doubtful.

A. Katz*'s Lack of Substance*

As described earlier, the reasoning and holding in *Katz* rested on three factors. First, the Court dismissed the importance of determining whether a telephone booth is a "constitutionally protected area."[108] Second, the Court rejected the "trespass" rule of prior cases.[109] Third, the Court emphasized the practical and vital role that public telephones play in private communications.[110] Taken together, these factors moved the Court to find that "a person in a telephone booth may rely upon the protection of the Fourth Amendment."[111] The factors cited in *Katz* lead to the sensible result that telephone conversations are entitled to constitutional protection.[112] But when these factors are removed from the facts in *Katz*, their usefulness for deciding the scope of the Fourth Amendment's protection in other

[108] *Katz*, 389 U.S. at 351.
[109] *Id.* at 352-53.
[110] *Id.* at 359.
[111] *Id.* at 352.
[112] *Id.* at 357.

contexts becomes illusory.

Consider, for example, *Katz*'s rejection of the litigants' efforts to determine whether a telephone booth was a "constitutionally protected area."[113] Justice Stewart asserted that focusing on whether a telephone booth is a constitutionally protected place "deflects attention from the problem presented by the case."[114] He then wrote his famous epigram: "[T]he Fourth Amendment protects people, not places."[115] This statement, while literally true, begs the question.[116] More importantly, asserting that the Amendment protects "people, not places," provides no guidance for determining, in *future cases*, when the Amendment protects people.[117] The emptiness of Justice Stewart's quip undoubtedly prompted Justice Harlan's clarification regarding the Amendment's scope. Justice Harlan noted that simply asserting "the Fourth Amendment protects people, not places" tells us nothing because the crucial question "is what protection it affords to those people."[118] According to Justice Harlan, "the answer to that question [generally] requires reference to a `place.'"[119] However, if one accepts Justice

---

[113] *Id.* at 351.

[114] *Id.*

[115] *Id.*

[116] *See, e.g.*, Amsterdam, *supra* note 23 at 385 (noting that the formula in *Katz* "begs the question. But I think it begs the question no more or less than any other theory of fourth amendment coverage the Court has used."). *See also* 1 LAFAVE, *supra* note 21, § 2.1(b) at 385. Professor LaFave remarks:

> [I]t can hardly be said that the [*Katz*] Court produced clarity where theretofore there had been uncertainty. If anything, the exact opposite has occurred. The pre-*Katz* rule, though perhaps `unjust,' was `a workable tool for the reasoning of the courts.' But the *Katz* rule, which the Court has since—somewhat inaccurately—stated as the `reasonable "expectation of privacy"' test, is by comparison `difficult to apply.' In short, the *Katz* `opinion offers little to fill the void it has thus created.'

1 LAFAVE, *supra* note 21, at 385 (footnotes omitted).

[117] *See, e.g.*, Clancy, *supra* note 1, at 339 (arguing that the *Katz* analysis has "no textual support in the language of the amendment" and thus "leaves the fluid concept of privacy to the vagaries of shifting Court majorities, which are able to manipulate the concept to either expand or contract the meaning of the word at will") (footnote omitted); Katz, *supra* note 104, at 559-60 ("[Justice Stewart's opinion] freed the [F]ourth [A]mendment from the chains imposed by the property limitation and the requirement of a physical trespass but provided modest guidance for determining the justiciability of an expectation of privacy in other contexts."). *Cf.* Ku, *supra* note 1, at 1346 (arguing that "by failing to provide any real guidance to the privacy value, [*Katz*] did not shut the door to examining [the means used by government agents], and subsequent decisions have taken advantage of this opening, artfully transforming the reasonable expectation of privacy test into a means-oriented analysis") (footnote omitted).

[118] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[119] *Id. See also* David A. Harris, *Superman's X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology*, 69 TEMP. L. REV. 1, 18 (1996) (explaining that after *Katz* "Fourth Amendment protection depends not only on

Harlan's reinterpretation of *Katz*, then, as Professor Sklansky observes, "the most famous words in *Katz* seem drained of most of their content."[120]

As Justice Harlan and others have recognized, *Katz*'s replacement for the concept of a "constitutionally protected area"—asserting that the "Fourth Amendment protects people, not places"—was a constitutional norm without substance. Because it is essentially meaningless, the norm that symbolizes the spirit and meaning of *Katz*, ironically, has proved to be quite ineffective, as a practical matter, in protecting people. *Katz*'s malleability and emptiness made it especially vulnerable in cases involving technological change. For example, within three years of the *Katz* decision, the Court confronted an issue that had divided the Justices in 1952. In *United States v. White*,[121] the Court had to decide whether the testimony of federal officers concerning conversations between the defendant and a government informant, which the officers monitoring the frequency of a radio transmitter that the informant carried overheard, implicated the Fourth Amendment.[122] Like *On Lee*, *White* ruled that the officers' electronic surveillance was not a search. Speaking for a plurality of the Court, Justice White explained the result with a syllogism: If a person assumes the risk that a secret government spy, acting without electronic equipment, might later reveal the contents of a conversation, the risk is the same when the spy simultaneously records and transmits the conversation to a government officer.[123] In both situations, "the risk is his," and the Fourth Amendment provides no protection against government conduct to obtain information in this manner.[124]

For the *White* plurality, *Katz* was irrelevant.[125] "Although

how an individual protects his privacy, but where and in what situation he does so").

[120] Sklansky, *supra* note 24 at 158; *cf.* Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1312 (noting that Justice Harlan's reformation of the rule of *Katz* "sits somewhat awkwardly alongside the majority opinion and makes it more difficult to give meaning to the vague `reasonable expectations of privacy' test).

[121] 401 U.S. 745 (1971).

[122] *White*, 401 U.S. at 746-47.

[123] *See id*. at 751-52 (plurality opinion).

[124] *Id*. at 752-53.

[125] Justice White distinguished *Katz* this way:

Katz involved no revelation to the Government by a party to

Katz announced that the Court would no longer be controlled by rigid and antiquated concepts when formulating the scope of the Fourth Amendment, the *White* plurality read *Katz* as having no impact on the secret spy cases"[126] decided before *Katz*. The *White* plurality, without any discussion or analysis of the doctrinal shift announced in *Katz*, reaffirmed prior holdings that authorized unchecked surveillance of private conversations and unbridled invasions of private homes and offices whenever informants are available to gather information for the government. If the "Fourth Amendment protects people, and not places," as *Katz* insisted, then why is the Amendment inapplicable against government efforts to record conversations or infiltrate homes or offices using secret informants?

> If the Fourth Amendment restrains the discretion of the police to wiretap or `bug' private conversations [conducted in telephone booths], it is not apparent why that same provision is inapplicable when the police monitor and record private conversations through the use of a secret informant deliberately position[ed] to hear those conversations. After all, a secret informant acts as a `human bug' for the government.[127]

The result in *White* proved that *Katz* offered no protection against this type of unchecked government electronic surveillance.

Katz's announcement that "the Fourth Amendment protects people, not places," also did not protect people from the unbridled use of electronic surveillance employed in *Smith v. Maryland*.[128] The question *Smith* presented was whether the installation and use of a pen register was a search under the Amendment.[129] The Court ruled that the pen register was not a search. *Smith* distinguished a pen register

---

> conversations with the defendant nor did the Court indicate in any way that a defendant has a justifiable and constitutionally protected expectation that a person with whom he is conversing will not then or later reveal the conversation to the police.

Id. at 749. Put simply, the Fourth Amendment does not cover eavesdropping by the government with the connivance of one of the parties.

[126] Tracey Maclin, *Informants and the Fourth Amendment*, 74 WASH. U. L. Q. 573, 620-21 (1996) (footnote omitted) [hereinafter Maclin, *Informants*].

[127] Maclin, *Informants*, *supra* note 126, at 625.

[128] 442 U.S. 735 (1979).

[129] The Court explained that a pen register "`is 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. It does not overhear oral communications and does not indicate whether calls are actually completed.'" *Smith*, 442 U.S. at 736, n.1 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 161, n.1 (1977)).

from wiretapping on several grounds.[130] The crux of the Court's logic, however, can be quickly summarized: The Fourth Amendment is not implicated because a person has no legitimate privacy interest in the telephone numbers he dials. The person assumes the risk that the telephone company will convey the numbers he dials to the government.

The Court was indifferent to the fact that technological innovations granted the government greater and more proficient access to information about a person's private communications.[131] In the Court's view, contemporary telephone equipment, including pen registers, is "merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber."[132] Noting that a person would have no legitimate privacy interest in the numbers he dialed if an operator processed those calls, the Court was "not inclined to hold that a different constitutional result is required because the telephone company has decided to automate."[133]

Smith did proclaim, unlike the *White* plurality, that *Katz* was its "lodestar" for determining whether government-initiated electronic surveillance triggered Fourth Amendment scrutiny.[134] But the protective shield of *Katz* was just as ineffective in *Smith* as it was in *White*. When *Katz* stated "the Fourth Amendment protects people, not places," criticism of this norm was muted because the majority of the Justices (like the majority of the nation) thought that private telephone conversations should be constitutionally protected. The emptiness of this norm, however, created a vacuum that the Court would have to fill in later cases where there was greater controversy about the challenged police practice. As

---

[130] *Smith* distinguished wiretapping from a pen register in the following ways. First, unlike a listening device, a pen register "do[es] not acquire the *contents* of communications." *Id.* at 741. Literally speaking, pen registers are not "recording devices" because they do not "`hear sound.'" *Id.* (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)). Furthermore, unlike listening devices, pen registers do not record "`any communication between the caller and the recipient of the call, [disclose the] identities [of the callers], [or tell] whether the call was even completed.'" *Id.*

[131] In his dissenting opinion, Justice Stewart notes that: "[t]he numbers dialed from a private telephone—although certainly more prosaic than the conversation itself are not without `content.'" *Id.* at 748 (Stewart, J., dissenting). Pen registers reveal, "the identities of the persons and the places called, and thus reveal the most intimate details of a person's life." *Id.* (Stewart, J., dissenting).

[132] *Id.* at 744.

[133] *Id.* at 745.

[134] *Id.* at 739.

those cases emerged, the Court needed legal theories to support controversial results that divided the Justices. The post-*Katz* Court used the expectations theory[135] and risk analysis to define the scope of the Fourth Amendment. The same assumption of risk theory supporting *White*'s holding supported *Smith*'s holding. As Justice Stewart belatedly recognized, however, "[i]t is simply not enough to say, after *Katz*, that there is no legitimate expectation of privacy in the numbers dialed because the caller assumes the risk that the telephone company will disclose them to the police."[136] Regrettably, Justice Stewart's realization came too late.[137] By 1979, *Katz*'s famous words were a meaningless slogan, often cited but lacking principle and influence. Expectations theory and risk analysis replaced *Katz* as the defining methodology

[135] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (explaining his view of the rule that has emerged through prior decisions is that "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as `reasonable'"). In *White*, Justice Harlan appeared to recant his endorsement of expectations theory as a tool for measuring the Fourth Amendment's scope. *See*, United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) (explaining that legal analysis in this context must "transcend the search for subjective expectations or legal attribution of assumptions of risk. Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present."); *see also*, Amsterdam, *supra* note 23, at 384 ("Justice Harlan himself later expressed second thoughts about [expectations theory], and rightly so. An actual, subjective expectation of privacy obviously has no place in a statement of what *Katz* held or in a theory of what the fourth amendment protects. It can neither add to, nor can its absence detract from, an individual's claim to fourth amendment protection.").

[136] *Smith*, 442 U.S. at 747 (Stewart, J., dissenting). Justice Stewart argued that *Smith*'s risk analysis was inconsistent with *Katz*. He also contended that risk analysis was a flawed legal theory because it proved too much. Telephone conversations:

> must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet we have squarely held that the user of even a public telephone is entitled `to assume that the words he utters into the mouthpiece will not be broadcast to the world.'

Id. at 746-47 (Stewart, J., dissenting) (quoting *Katz*, 389 U.S. at 352). Why shouldn't a caller assume the risk that his conversation may be turned over to the government, just as the numbers he dials may be conveyed to the government? People do not assume *that* risk, or assume the risk that our mail may be opened and read by government officers, because the Court has said we do not have to assume those risks. Risk analysis is not based on a neutral principle. We assume only those risks the Court says we must assume. *See* KAMISAR ET AL., *supra* note 18 at 380 (citation omitted) (noting that we do not assume the risk that our telephone calls or mail is being monitored because the Court has ruled that the government may not conduct such surveillance).

[137] Interestingly, Justice Stewart had joined the plurality opinion in *White* which, as noted in the text, relied on the assumption of risk theory to support the holding. *See generally White*, 401 U.S. at 745-54 (plurality opinion).

for measuring the Fourth Amendment's protection.[138]

The second factor supporting *Katz*'s reasoning and holding adopted the view that "the reach of [the Fourth Amendment] cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[139] Rejection of the "trespass" rule heralded a new model of search and seizure jurisprudence.[140] Common-law property rules would no longer dominate the debate about the scope and meaning of the Fourth Amendment. Without being tethered to archaic rules, the Court was free to conduct a modern and realistic assessment about which police practices should be subject to constitutional scrutiny. But loosening the connection between search and seizure law and common-law rules did not enhance *Katz*'s authority to protect Fourth Amendment interests in future cases. Indeed, besides the outcome in *Katz* itself, rejection of the trespass rule rarely made a difference in search and seizure rulings.

Rejection of the "trespass" rule ignited no real

---

[138] *See* United States v. Miller, 425 U.S. 435 (1976). *Miller* ruled that a government subpoena of bank checks and deposit slips from banks did not constitute a search. The Court explained that the "depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *Id.* at 443. The "assumption of risk" rule applies "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in third party will not be betrayed." *Id.* For a detailed discussion of the Court's analysis in *Smith*, see Clifford S. Fishman, *Pen Registers and Privacy: Risks, Expectations, and the Nullification of Congressional Intent*, 29 CATH. U. L. REV. 557, 561 (1980) (noting that "[a]lthough the result in *Smith* is supportable under the particular facts of the case, the Court's reasoning poses significant problems of both statutory and constitutional dimensions"); *id.* at 569 (asserting that *Smith*'s "reliance on *Miller* to support an assumption of risk rationale in the context of electronic surveillance is rather tenuous"). Professor Daniel Solove describes the constitutional framework established by risk analysis as the "new *Olmstead*."

> Although we have moved from the *Boyd [v. United States*, 116 U.S. 616 (1886)] and *Olmstead* world of physical papers and places to a new regime based upon expectations or privacy, there is a new *Olmstead*, one that is just as shortsighted and rigid in approach. The Court's new conception of privacy is one of total secrecy. If any information is exposed to the public or if law enforcement officials can view something from any public vantage point, then the Court has refused to recognize a reasonable expectation of privacy.

Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1133 (2002).

[139] *Katz*, 389 U.S. at 353.

[140] *See, e.g.*, LAFAVE, *supra* note 21, § 2.2 (c) at 418 (describing *Katz*'s disapproval of the trespass rule as a "dramatic shift [which] made it quite clear that the earlier [lower court] decisions upholding the use of telescopic devices by reliance upon *Goldman* [*v. United States*, 316 U.S. 129 (1942)] and *Hester* [*v. United States*, 265 U.S. 57 (1924)] could no longer be safely relied upon").

controversy among the Justices in *Katz*.[141] One explanation for this consensus may be that the trespass rule specifically, and common-law property rules generally, no longer exerted influence on search and seizure doctrine. Since at least the 1950's, the persuasive quality of these rules waned. "The validity of the trespass rationale was questionable even at the time [*On Lee*] was rendered" in 1952.[142] Rulings subsequent to *On Lee* further eroded the property-based foundations of Fourth Amendment law.[143] As Justice Harlan explained, search and seizure doctrine immediately prior to *Katz* demonstrated "no tolerance for the old dividing lines resting, as they did, on fiction and common-law distinctions without sound policy justification in the realm of values protected by the Fourth Amendment."[144] Under this view, the *Katz* opinion, rather than initiating a fundamental shift, was merely a final and formal acknowledgement that the trespass rule had outlived its usefulness.[145]

Moreover, the trespass or physical penetration concept was quickly becoming obsolete. Technological change was allowing government officials to obtain information without physical intrusions into constitutionally protected areas. Dog sniffs, airplanes and electronic beepers were a small sample of the types of technological advances that enabled the government to obtain information without physical intrusion. When litigants raised constitutional challenges against these investigative devices, the Court responded as if it had not

---

[141] Even Justice Black, the sole dissenter in *Katz*, did not object when the Court jettisoned the trespass rule. *See Katz*, 389 U.S. at 368-69 (Black, J., dissenting) (explaining that the presence or absence of a trespass was not determinative in the pre-*Katz* cases).

[142] *White*, 401 U.S. at 774 (Harlan, J., dissenting); *see also*, Katz, *supra* note 104 at 558 (noting that by 1960, dissatisfaction with the trespass doctrine was being expressed within the Court and by legal academics).

[143] *See, e.g.*, Warden v. Hayden, 387 U.S. 294 (1967). Seven months prior to *Katz*, *Hayden* stated:

> The premise that property interests control the right of the Government to search and seize has been discredited. Searches and seizures may be `unreasonable' within the Fourth Amendment even though the Government asserts a superior property interest at common law. We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts.

Hayden, 387 U.S. at 304 (citing Jones v. United States, 362 U.S. 257, 266 (1960) and Silverman v. United States, 365 U.S. 505, 511 (1961)).

[144] *White*, 401 U.S. at 778 (Harlan, J., dissenting).

[145] *Cf.*, *id.* at 780 (Harlan, J., dissenting) ("Viewed in perspective, then, *Katz* added no new dimension to the law. At most it was a formal dispatch of *Olmstead* and the notion that such problems may usefully be resolved in the light of trespass doctrine, and, of course, it freed from speculation what was already evident, that *On Lee* was completely open to question.").

decided *Katz*. For example, in *United States v. Place*,[146] the Court concluded that exposing personal luggage to a narcotics detection dog was not a "search."[147] *Place* concluded "the canine sniff is *sui generis*."[148] It does not "require opening the luggage" and "discloses only the presence or absence of narcotics, a contraband item."[149]

The analytical tension between *Place* and *Katz* is manifest. Why does it matter that the dog sniff does not require opening of luggage? After all, *Place* recognized that "a person possesses a privacy interest in the contents of personal luggage that is protected by the Fourth Amendment,"[150] and conceded that "the sniff tells the authorities something about the contents of the luggage, [although] the information . . . is limited."[151] The absence of a physical intrusion does not diminish a person's privacy interest in his luggage, just as the absence of a physical intrusion into a telephone booth did not diminish Katz's interest in the privacy of his telephone conversations. More importantly, *Katz* instructed that Fourth Amendment protection does not turn on the presence or absence of a physical intrusion. Thus, the "manner" of the police intrusion

---

[146] 462 U.S. 696 (1983).

[147] *Place*, 462 U.S. at 707.

[148] *Id*. Not surprisingly, "canine sniffs turned out not to be *sui generis* at all." Harris, *supra* note 119, at 30, n.177. The next year, in *United States v. Jacobsen*, 466 U.S. 109 (1984), the Court employed the logic of *Place* to find that a chemical field test of powdery substance did not constitute a search. Because the chemical test—like the canine sniff—only revealed whether the powder was cocaine or not, no Fourth Amendment interests were triggered. *Jacobsen* 466 U.S. at 123-24. "The [*Jacobsen*] Court also extended the reach of *Place*, by saying that the search not only disclosed a limited *amount* of information, but also that it disclosed only a *type* of information—the presence of absence of cocaine—*in which there could be no legitimate expectation of privacy*." Harris, *supra* note 119, at 31.

[149] *Place*, 462 U.S. at 707. *Place* explained that because there was no physical intrusion, the dog sniff "does not expose noncontraband items that otherwise would remain hidden from public view, as does, for example, an officer's rummaging through the contents of the luggage. Thus, the manner in which information is obtained through this investigative technique is much less intrusive than a typical search." *Id*.

[150] *Id*. at 707 (citing United States v. Chadwick, 433 U.S. 1, 13 (1977)).

[151] *Id*. As Professor Harris has noted, the canine sniff does not simply augment human capabilities.

> Although both man and dog can smell, the dog's nose was not simply a way to enhance what the human at the end of the leash could do. Rather, the canine nose is so much better-more sensitive and more accurate—than its human counterpart that it simply could not be said to replace it.

Harris, *supra* note 119 at 24, n.137.

in *Place* should be irrelevant.

Likewise, *California v. Ciraolo*[152] held that naked-eye aerial observation of an individual's backyard did not constitute a search.[153] Writing for a five Justice majority, Chief Justice Burger asserted no search occurred because the police observations "took place within public navigable airspace" in a "physically nonintrusive manner."[154] Again, *Katz*'s impotence was evident. The dissent charged that the Chief Justice had ignored fundamental elements of *Katz*'s reasoning.[155] Rather than address the obvious tension between his reasoning and *Katz*, the Chief Justice essentially confined the reach of *Katz* to a privilege against warrantless wiretapping.[156] According to the Chief Justice, the concerns of the *Katz* majority and Justice Harlan focused on electronic interception of telephone communications. "One can reasonably doubt that in 1967 [the Justices of *Katz*] considered an aircraft within the category of future `electronic' developments that could stealthily intrude upon an individual's privacy."[157] Once the Chief Justice disabled *Katz* in this way, it was easy to conclude that the Fourth Amendment does not bar naked eye aerial observation of a person's backyard.

Finally, the result and reasoning of *United States v. Knotts*[158] reveals the insignificance of *Katz*'s proclamation that the Fourth Amendment's reach "cannot turn upon the presence of absence of a physical intrusion into any given

---

[152] 476 U.S. 207 (1986).

[153] *Ciraolo*, 476 U.S. at 213-14.

[154] *Id.* at 213.

[155] Justice Powell's dissent in *Ciraolo* complained that the majority was ignoring Justice Harlan's warning that any "decision to construe the Fourth Amendment as proscribing only physical intrusions by police onto private property `is, in the present day, bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion.'" *Id.* at 215-16 (Powell, J., dissenting) (quoting *Katz*, 389 U.S. at 362 (Harlan, J., concurring)). Justice Powell also noted that the *Ciraolo* majority's reliance on the fact that the flyover was conducted in a physically nonintrusive manner directly contradicted *Katz*.

> Reliance on the *manner* of surveillance is directly contrary to the standard of *Katz*, which identifies a constitutionally protected privacy right by focusing on the interests of the individual and of a free society. Since *Katz*, we have consistently held that the presence or absence of physical trespass by police is constitutionally irrelevant to the question whether society is prepared to recognize an asserted privacy interest as reasonable.

Id. at 223 (Powell, J., dissenting) (citation omitted).

[156] *See id.* at 214.

[157] *Id.* at 215.

[158] 460 U.S. 276 (1983).

enclosure."[159] *Knotts* was the Court's first "beeper" case.[160] Law enforcement officers installed a beeper in a drum of chloroform that one of the defendants purchased in Minnesota. Visual and electronic surveillance enabled officers to monitor the whereabouts of the drum as it traveled from Minnesota to Wisconsin. The officers eventually discovered that the beeper signal was stationary and situated near a secluded cabin. A subsequent search of the cabin pursuant to a warrant, based in part on the information the officers had obtained while monitoring the beeper, disclosed a drug laboratory. The issue in *Knotts* was whether the monitoring was a search. Relying upon the lesser expectation of privacy associated with cars, *Knotts* first stated that a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[161]

The Court then addressed whether the use of electronic detection equipment triggered Fourth Amendment interests. As in the other post-*Katz* cases that posed conflicts between technology and Fourth Amendment rights, the *Knotts* Court did not see *Katz*'s reasoning as placing any constitutional restraints on police use of beepers. In fact, *Knotts*'s logic proceeded as if the Court had never heard of *Katz*. According to then-Justice Rehnquist, the author of *Knotts*, "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[162] This statement, however, contradicts *Katz* itself.[163]

---

[159] *Katz*, 389 U.S. at 353.

[160] The Court described the "beeper" as "a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver." *Knotts*, 460 U.S. at 277. The Court's second beeper case was *Karo v. United States*, 468 U.S. 705 (1984). For a comprehensive and informative analysis of *Knotts* and *Karo*, see Clifford S. Fishman, *Electronic Tracking Devices and the Fourth Amendment*: Knotts, Karo, *and the Questions Still Unanswered*, 34 CATH. U. L. REV. 277 (1985); Melvin Gutterman, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 SYRACUSE L. REV. 647, 699-707 (1988).

[161] *Knotts*, 460 U.S. at 281.

[162] *Id.* at 282.

[163] *See id.* at 288 (Stevens, J., concurring). In *Knotts*, Justice Stevens stated that the electronic augmentation "was unobjectionable, [but] it by no means follows that the use of electronic detection techniques does not implicate especially sensitive concerns." *Id.* Professor Fishman, who generally supports the result in *Knotts*, agrees with Justice Stevens' concern that sense-enhancement

Under Justice Rehnquist's reasoning, the Fourth Amendment provides no protection against electronic or technological devices that enhance human senses, even when electronic surveillance is indispensable to the government's ability to gather information. Because the officers in *Knotts* were *unable* to maintain visual surveillance of the drum as it traveled from Minnesota to Wisconsin, the beeper allowed them to locate the chloroform "when they would not have been able to do so had they relied solely on their naked eyes."[164] Justice Rehnquist, however, concluded that "scientific enhancement of this sort raises no constitutional issues which visual surveillance would not also raise."[165] In other words, because an officer in a car (or in a helicopter)[166] theoretically could have maintained visual observation of the drum as it traveled across the country without triggering constitutional protection, no constitutional concerns are raised if that officer utilizes electronic equipment to accomplish the same task.

In a technologically advanced society, acceptance of Justice Rehnquist's rationale in *Knotts*—equating electronic surveillance with what police might theoretically accomplish with naked eye monitoring—means that the Fourth Amendment will protect very little.[167] In the theoretical world, one can always imagine methods in which the police are able to watch, listen, or even smell, the activities of a suspect in order to detect useful information. In the real

equipment raise especially sensitive issues. Fishman, *supra* note 160, at 323. But Professor Fishman also believes that the *Knotts* majority was aware of the potential dangers posed by technological enhancement, and thus wrote a narrow opinion that authorized only the specific surveillance at issue in that case. Fishman, *supra* note 160, at 323.

[164] *Knotts*, 460 U.S. at 285. *Cf.* Fishman, *supra* note 160, at 324, n.194 (acknowledging that the police did not learn of the defendant's destination by visual surveillance).

[165] *Knotts*, 460 U.S. at 285.

[166] At one point in their surveillance of the defendant's automobile, the defendant took evasive action and the officers ended their visual surveillance. "At about the same time officers lost the signal from the beeper, but with the assistance of a monitoring device located in a helicopter the approximate location of the signal was picked up again about one hour later." *Knotts*, 460 U.S. at 278.

[167] Professor LaFave's reaction to *Knotts* has been more polite. "It is this assumed equivalence between mere `visual surveillance' and `scientific enhancement' in *Knotts* which is troublesome." LAFAVE, *supra* note 21, §2.7(e) at 645. Professor LaFave properly notes what Justice Rehnquist refused to admit: "The use of an electronic tracking device permits a much more extended and thorough surveillance of an individual than would otherwise be possible." LAFAVE, *supra* note 21, §2.7(e) at 645. *Cf.* Ku, *supra* note 1, at 1348 (noting that the practical impact of *Knotts* allows "government to monitor any individual outside of the home twenty-four hours a day without any discussion of how that monitoring might affect the individual or what that surveillance might do to the relationship between government and individual") (footnote omitted).

world, however, police investigative methods are subject to financial, personnel and political restraints. The scope of the Fourth Amendment should not be measured by a judge's ability (or inability) to conjure hypothetical scenarios in which an individual's activities are monitored by police who are able to "augment[] the sensory faculties bestowed upon them at birth with such enhancement as science and technology" permits.[168] Otherwise, very few human activities will be beyond the government's surveillance capabilities.

The leeway given the police under *Knotts*'s reasoning is illustrated by applying *Knotts*'s rationale to a "hypothetical" *Katz* case. Under *Knotts*'s logic, the result in *Katz* is uncertain.[169] Conceivably, lip-reading FBI agents could watch and transcribe what they saw as Katz spoke in a glass enclosed phone booth. If Katz became aware of the agents' presence and covered his lips, presumably, under the analysis of *Knotts*, the agents could turn on a wiretap to augment their sensory faculties without triggering Fourth Amendment scrutiny. Just as the officers in *Knotts* used electronic equipment—without triggering constitutional safeguards—to discover the location of the chloroform "when they would not have been able to do so had they relied solely on their naked eyes,"[170] lip-reading FBI agents could have also used electronic surveillance to ascertain Katz's communications when they "would not have been able to do so had they relied solely on their naked eyes."[171] In either case, "[n]othing in the Fourth Amendment prohibited the police [or FBI] from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afford[s]."[172] As Justice Rehnquist suggested in *Knotts*, "scientific enhancement of this sort raises no constitutional issues which

---

[168] *Knotts*, 460 U.S. at 282.

[169] *Cf.* 1 LAFAVE, *supra* note 21, § 2.7(e) at 646, n.114 ("[A] *Smith-Knotts* type of analysis could well have produced the result that Katz lacked an expectation of privacy because what he said could have been determined by a lip reader some distance away or by a hypothetical bystander immediately adjacent to the booth.").

[170] *Knotts*, 460 U.S. at 285.

[171] *Id*. *See also* JOSHUA DRESSLER & GEORGE C. THOMAS III, CRIMINAL PROCEDURE: PRINCIPLES, POLICIES AND PERSPECTIVES 88 (1999) (asking whether the result in *Katz* would be the same if FBI agents "had positioned a lip reader immediately outside the telephone booth who observed Katz's lips and recorded his words on paper").

[172] *Knotts*, 460 U.S. at 282.

visual surveillance would not also raise."[173] At bottom, *Knotts*'s reasoning raises doubts about the protection that *Katz* provided.[174]

As in *Smith v. Maryland*, *Place* and *Ciraolo*, the reasoning of *Knotts* shows that *Katz*'s rejection of the trespass rule has had little impact on subsequent search and seizure cases involving technological and scientific innovations. Before it was finally overruled, the trespass rule had lost its influence among the Justices. Even if *Katz* had not reversed the trespass rule, law enforcement investigative methods, with the aid of technology, were advancing at such a rapid pace that the government could obtain various types of information without a physical intrusion into a constitutionally protected area. Thus, *Katz*'s proclamation on this point was meaningless, and the Court's later decisions would show that *Katz*'s reasoning would matter little when police utilized

---

[173] *Id.* at 285.

[174] Professor Fishman does not agree with this criticism of *Knotts*. *See* Fishman, *supra* note 160, at 325. He notes:

> Surveillance of one's location and surveillance of one's words differ, not merely in degree, but in kind. Under most circumstances, a person's location and travel simply are not `private,' and surveillance, though potentially offensive, does not intrude as deeply or as dangerously into privacy and individual liberty as does surreptitious surveillance of what one says to friends, relatives and other confidants. Thus, it is not at all inconsistent for the Court to have held that electronic surveillance of communications is a search subject to Fourth Amendment protection, while also holding that electronic surveillance of public travel is not.

Fishman, *supra* note 160, at 325 (footnote omitted). While reasonable minds might agree that the "location" surveillance in *Knotts* is not as intrusive as the communication surveillance in *Katz*, my criticism of *Knotts* is not focused on the *degree* or intrusiveness of the surveillance involved in that case. Rather, my point is to highlight the contrasting analytical methods between *Knotts* and *Katz*. As noted in the text, *Knotts*'s analysis gives the police enormous latitude to monitor the activities of individuals. In some cases, the surveillance will be quite intrusive, as in the example of the lip-reading FBI agents who augment their sensory faculties with electronic equipment. In other cases, the surveillance may be insignificant, as Justice Stevens believed to be the case in *Kyllo*. *See* Kyllo v. United States, 533 U.S. 27, 43 (2001) (Stevens, J., dissenting) (noting that "the ordinary use of the senses might enable a neighbor or passerby to notice the heat emanating from a building"); *Kyllo*, 533 U.S. at 45 (arguing that police "should not have to avert their senses or their [sense-enhancing] equipment from detecting emissions in the public domain," particularly when "the countervailing privacy interest is at best trivial"). In a third group of cases, reasonable minds might disagree about the intrusiveness involved when government officers are free to augment their sensory faculties with enhancement by scientific and technological devices. *Compare Smith v. Maryland*, 442 U.S. 735, 741 (opinion of Blackmun, J.) *with Smith*, 422 U.S. at 746-48 (opinion of Stewart, J., dissenting). In sum, the problem with the Court's analysis in *Knotts* is that it proves too much. Under *Knotts*'s logic, the Fourth Amendment will be inapplicable if the government can convince a judge that the information revealed by the technological or scientific intrusion *could have* been detected by officers combining sense-enhancing equipment with their ordinary human senses.

other types of technological tools to gather information.

The third and final factor that *Katz* emphasized was that "[o]ne who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[175] *Katz* explained that the warrantless wiretap violated "the privacy upon which [Katz] justifiably relied while using the telephone booth and thus constituted a `search and seizure' within the meaning of the Fourth Amendment."[176]

This aspect of *Katz* is nearly impossible to administer. As Professor LaFave comments, the "expectation" formula of *Katz* does not produce "clarity where theretofore there had been uncertainty. If anything, the exact opposite has occurred."[177] The rest of the *Katz* opinion, as the above discussion demonstrates, provides scant guidance on explaining when other individuals can "justifiably rel[y]" on the Fourth Amendment to protect them from warrantless government surveillance.[178] In sum, because it lacks any type of principled norm, the expectations test, like the other two factors that *Katz* emphasized, does not provide a substantive model or neutral principle that protects Fourth Amendment liberties.

---

[175] Katz v. United States, 389 U.S. 347, 352 (1967).

[176] *Id.* at 353.

[177] 1 LAFAVE, *supra* note 21, § 2.1(b) at 385.

[178] *See supra* note 174 and accompanying text; *see also, Kyllo*, 533 U.S. at 34 (noting that *Katz*'s expectations test "has often been criticized as circular, and hence subjective and unpredictable") (citations omitted); LAFAVE, *supra* note 21, § 2.1(b) at 386 (explaining that "[a]lthough *Katz* unquestionably expands the coverage of the Fourth Amendment, even now—despite the intervening years since *Katz* was handed down—it is impossible to state with precision the degree of this expansion"); Gutterman, *supra* note 160, at 665 (noting that "[g]overnment conduct could be insulated from [constitutional] review when the precautions taken were not weighted sufficiently to earn privacy. The *Katz* promise had sowed its own seeds of destruction.") (footnote omitted); *cf.* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 63 (Random House 2000) ("[T]he real problem with the Supreme Court's test for invasions of privacy is not empirical but conceptual. In many cases, people have an objectively valid expectation of privacy that the Court, by judicial fiat, has deemed unjustifiable.").

B. The Justices Themselves Could Not Agree On

The Meaning of Katz

Because the three factors critical to the result in *Katz* were meaningless or insignificant, it is not surprising that *Katz* has been ineffective in protecting Fourth Amendment interests in cases not involving wiretapping or electronic bugging of private conversations. But the emptiness of these factors was not the only problem with *Katz.* Another flaw in *Katz,* although not immediately apparent in the Court's opinion, was the fact that the Justices who joined the result in *Katz* could not agree on its meaning. The inability of the Justices who decided *Katz* to agree on the scope and impact of their own decision diminished any expectation that *Katz* could have a lasting impact on Fourth Amendment liberties. Indeed, the discord over *Katz,* when combined with the emptiness of its legal framework, only increased the chances that future Justices would see *Katz* as a narrow precedent regarding the Fourth Amendment's scope in a scientific and technologically advanced society.

Although few would realize the point until much later, the scope of *Katz*'s holding was in doubt on the day the Court rendered its decision. In his concurring opinion, Justice White asserted that *Katz* left undisturbed a line of cases dealing with informants and wired spies.[179] According to Justice White, when a person speaks to another, the speaker "takes all the risks ordinarily inherent in so doing, including the risk that the man to whom he speaks will make public what he has heard."[180] The Fourth Amendment affords no protection against "unreliable (or law-abiding) associates."[181] A sensible extension of this rule, according to Justice White, leads to the conclusion that a speaker also assumes the risk "that his hearer, free to memorize what he hears for later verbatim repetitions, is instead recording it or transmitting it to another."[182] *Katz,* on the other hand, dealt with "an entirely different situation" because Katz attempted to exclude uninvited listeners and "spoke under circumstances in which a reasonable person would assume that uninvited ears were not listening."[183]

---

[179] *Katz,* 389 U.S. at 363, n.* (White, J., concurring).
[180] *Id.* (White, J., concurring).
[181] *Id.*
[182] *Id.*
[183] *Id.*

Justice White's comments sought to bolster the "assumption of risk" analysis that supported *On Lee*. When *Katz* was decided, no member of the *Katz* majority challenged Justice White's interpretation of *Katz*'s holding. Four years later, however, an influential member of the *Katz* majority challenged Justice White's understanding of *Katz*'s impact on the wired spy cases. Justice Harlan, the author of what later became known as the "*Katz* analysis"[184] or "*Katz* test,"[185] disputed Justice White's interpretation of *Katz* in *United States v. White*.[186] On this occasion, however, Justice White's views on *Katz*'s meaning would prevail over the views of Justice Harlan.

White reaffirmed *On Lee*'s holding that governmental use of a wired spy to record the conversations of an individual is not a search under the Fourth Amendment. As noted earlier, Justice White's plurality opinion in *White* relied upon the assumption of risk theory to explain why an individual has no constitutionally protected interests against government use of wired informants. Not surprisingly, Justice White read *Katz*'s holding, as he did in his concurring opinion in *Katz*, as not affecting the rationale supporting *On Lee* or *Lopez*.[187] In contrast, Justice Harlan's dissent in *White* argued that subsequent cases had eroded the "doctrinal foundations" of *On Lee*. According to Justice Harlan, *Katz*, in combination with other rulings decided in the 1960's, not only expunged the property-law doctrine that previously controlled the results in search and seizure cases, it also cast serious doubt on the continuing validity of cases like *On Lee* and *Lopez*.[188] The reasoning in *Katz*, following closely on the heels of *Berger*, signaled a heightened judicial awareness of the dangers that technology posed to individual privacy. Indeed, even without *Katz*, the Court had already changed direction on the constitutionality of electronic surveillance.

---

[184] Smith v. Maryland, 442 U.S. 735, 741 (1979) (referring to Justice Harlan's concurrence in *Katz* which established a two-part test for determining when a "search" occurred, as "the *Katz* analysis").

[185] Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (commenting on "the *Katz* test (which has come to mean the test enunciated by Justice Harlan's separate concurrence in *Katz*)").

[186] 401 U.S. 745 (1971).

[187] Justice White distinguished *Katz* by explaining that:

> *Katz* involved no revelation to the Government by a party to conversations with the defendant nor did the Court indicate in any way that a defendant has a justifiable and constitutionally protected expectation that person with whom he is conversing will not then or later reveal the conversation to the police."

White, 401 U.S. at 749 (plurality opinion).

[188] *Id.* at 776-80 (Harlan, J., dissenting).

Specifically, Justice Harlan noted that *Berger* "expressed concern about scientific developments that have put within the reach of the Government the private communication of `anyone in almost any given situation,' [and] it left no doubt that, as a general principle, electronic eavesdropping was an invasion of privacy and that the Fourth Amendment prohibited unsupervised `bugging.'"[189] In Justice Harlan's view, *Katz* was simply the concluding chapter of the Court's new edition on the meaning of the Fourth Amendment.

Justices White and Harlan not only proffered different views on *Katz*'s specific holding, they also differed on *Katz*'s impact on Fourth Amendment theory. For Justice White, *Katz*'s impact was limited to overruling the trespass rule. *Katz* did not affect the assumption of risk theory of prior cases, nor did it represent a shift in judicial analysis in determining the Fourth Amendment's reach.[190] Justice Harlan, on the other hand, questioned the compatibility of "risk analysis" and "expectations" theory with the Court's contemporary approach to defining the Fourth Amendment's reach. Although his opinions in *Lopez* and *Katz* were crucial to the development of each of these legal theories, Justice Harlan now believed that risk analysis and expectations theory was neither consistent with the holding of *Katz* nor compatible with the central purpose of the Amendment.[191] Justice Harlan's comments seem to recognize that the analysis of *Katz*—relying as it does on the individual's expectations—was an inadequate model for defining the Fourth Amendment's reach in an age of technological innovation. For Harlan, merely describing the risks a person assumes or subjective expectations he holds was a flawed model for identifying the Fourth Amendment's reach. The "critical question" was whether the Court "should impose on

---

[189] *Id.* at 779 (Harlan, J., dissenting) (quoting Berger v. New York, 388 U.S. 41, 47 (1967)).

[190] Justice White saw no constitutional difference between wired and unwired spies.

> Given the possibility or probability that one of his colleagues is cooperating with the police, it is only speculation to assert that the defendant's utterances would be substantially different or his sense of security any less if he also thought it possible that the suspected colleague is wired for sound.

White, 401 U.S. at 752 (plurality opinion). According to Justice White, government use of wired and unwired informants "is ruled by fluid concepts of `reasonableness.'" *Id.* at 753 (plurality opinion).

[191] *See id.* at 786 (Harlan, J., dissenting).

our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement."[192] Unlike Justice White, who thought that a traditional "reasonableness" model was capable of assessing the constitutionality of electronic surveillance, Justice Harlan appeared to be saying that the Court must go further than simply asking what constitutes reasonable police conduct. Instead, the Justices must examine "the realm of values protected by the Fourth Amendment."[193]

A second illustration of the Court's internal discord over the meaning of *Katz* occurred in the term following *Katz*. In *Desist v. United States*,[194] the Court had to decide whether *Katz*'s holding should be given retrospective application. When *Desist* was decided, one of the criteria for determining whether a new constitutional ruling would be given retroactive affect focused on "the extent of the reliance by law enforcement authorities on the old standards."[195] With this concern in mind, the defendants in *Desist* argued that *Katz* "merely confirmed the previous demise of obsolete decisions enunciating the distinction between `trespassory' searches and those in which there was no physical penetration of the protected premises."[196] The *Desist* Court, however, concluded that this argument "misconstrues our opinion in *Katz*."[197] According to Justice Stewart, the author of *Desist*, on the day the Court decided *Katz*, "the assumption persisted that electronic surveillance did not offend the Constitution unless there was an `actual intrusion into a constitutionally protected area.'"[198] Justice Stewart conceded that decisions which preceded *Katz* "may have reflected growing dissatisfaction with the traditional tests of the constitutional

---

[192] *Id*.

[193] *Id*. at 778; *see also id*. at 786-87 (arguing that the Court must assess "the nature of a particular [police] practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement. For those more extensive intrusions that significantly jeopardize the sense of security which is the paramount concern of Fourth Amendment liberties, I am of the view that more than self-restraint by law enforcement officials is required and at the least warrants should be necessary.") (citations omitted).

[194] 394 U.S. 244 (1969).

[195] *Desist*, 394 U.S. at 249 (quoting Stovall v. Denno, 388 U.S. 293, 297 (1967)). The other two criteria were: "the purpose to be served by the new standards" and "the effect on the administration of justice of a retroactive application of the new standards." *Id*. The legal standards for retroactive application of Supreme Court precedents have changed since *Desist* was decided. *See* KAMISAR ET AL, *supra* note 18, at 41-47.

[196] *Desist*, 394 U.S. at 247 (citations omitted).

[197] *Id*.

[198] *Id*. at 248.

validity of electronic surveillance," but he noted that the Court had never overruled those tests.[199] Thus, while the result in *Katz* "may have been foreshadowed, it was a clear break with the past."[200] Accordingly, *Desist* ruled that *Katz* would have only prospective application.

This understanding of *Katz* baffled Justice Fortas, who had joined Justice Stewart's majority opinion in *Katz* itself. Justice Fortas was certain that the trespass rule was dead long before the *Katz* decision.[201] But another aspect of the Court's failure to apply *Katz* retrospectively troubled Justice Fortas. He noted that the "vitality of our Constitution depends upon conceptual faithfulness and not merely decisional obedience" that law enforcement officials and lower courts afford to the Court's precedents.[202] By giving *Katz* only prospective application, the *Desist* Court sent two related messages to police officials and lower court judges. One message encouraged police officials "who honor the Constitution's mandate only where acceptable to them or compelled by the precise and inescapable specifics of a decision of this Court."[203] The second message that *Desist* sent was more pointed. Prospective application of *Katz* awarded

> dunce caps to those law enforcement officers, courts, and public officials who do not merely stand by until an inevitable decree issues from this Court, specifically articulating that which is clearly immanent in the fulfillment of the Constitution, but who generously apply the mandates of the Constitution as the developing case law elucidates them.[204]

Justice Fortas's comments on the importance of "conceptual faithfulness" to Supreme Court precedents help to identify a basic problem with *Katz*. Justice Fortas's dissent in *Desist* was a veiled criticism of law enforcement officers and judges who took a narrow view of the Court's pre-*Katz*

---

[199] *Id.*

[200] *Id.*

[201] Using somewhat colorful language, Justice Fortas stated:

> *Katz* is not responsible for killing *Olmstead*. Prior cases had left the physical-trespass requirement of *Olmstead* virtually lifeless and merely awaiting the death certificate that *Katz* gave it. They demonstrated to all who were willing to receive the message that *Olmstead* would not shield eavesdropping because it took place outside the physical property line.

Desist, 394 U.S. at 275 (Fortas, J., dissenting) (citations omitted).

[202] *Id.* at 277.

[203] *Id.*

[204] *Id.*

cases. Some of the conservative Justices of the Burger and Rehnquist Courts have encountered similar criticism for their application of *Katz*.[205] But before police officers, lower court judges, and even Supreme Court Justices can be expected to honor the "conceptual faithfulness" of a Court ruling, they have to know what that ruling requires of them. The problem with *Katz* is that it was so lacking in substance and subject to judicial manipulation that it could mean anything to anyone.

The debate between Justices White and Harlan in *White* and Justices Stewart and Fortas in *Desist* illustrate the problem that occurs when the Justices who decide a "landmark" case like *Katz* disagree among themselves. For example, when the Justices cannot agree whether a case fundamentally altered the "rules of the game" regarding the constitutionality of electronic surveillance,[206] that case is an unlikely protector of civil liberties in future cases involving technological and scientific innovations that threaten Fourth Amendment rights. Similarly, if within a year's time, the Justices who announce a ruling that many legal scholars characterize as a revolutionary alteration of the protection provided by the Fourth Amendment are deeply divided over whether that ruling "was a clear break with the past," then that ruling should not be expected to generate consensus among future Justices regarding its meaning in other constitutional contexts. Despite the apparent consensus among the Justices when they decided *Katz*, it soon became obvious that the same Justices who participated in the *Katz*

---

[205] *See, e.g.*, Minnesota v. Carter, 525 U.S. 83, 110-11 (1998) (Ginsburg, J., dissenting) ("The Court's decision in this case veers sharply from the path marked in *Katz*."); Florida v. Riley, 488 U.S. 445, 456 (1989) (Brennan, J., dissenting) ("The opinion for a plurality of the Court reads almost as if [*Katz*] had never been decided."); *id.* at 457 (plurality's position that helicopter surveillance of a backyard is not a search "ignores the very essence of *Katz*"); California v. Ciraolo, 476 U.S. 207, 216 (1985) (Powell, J., dissenting) (asserting that the Court "departs significantly from the standard developed in *Katz*"); Oliver v. United States, 466 U.S. 170, 188 (1984) (Marshall, J., dissenting) ("The Court's contention that, because a field is not a house or effect, it is not covered by the Fourth Amendment is inconsistent with th[e] [*Katz*] line of cases and with the understanding of the nature of constitutional adjudication from which it derives.") (footnote omitted).

[206] *Compare* United States v. White, 401 U.S. 745, 750 (1971) (plurality opinion of White, J.) ("We see no indication in *Katz* that the Court meant to disturb [the "risk analysis" theory] or to disturb the result reached in the *On Lee* case, nor are we now inclined to overturn this view of the Fourth Amendment.") (footnote omitted), *with White*, 401 U.S. at 780 (opinion of Harlan, J., dissenting) (stating that *Katz* "added no new dimension to the law. At most it was a formal dispatch of *Olmstead* and the notion that such problems may usefully be resolved in the light of trespass doctrine, and, of course, it freed from speculation what was already evident, that *On Lee* was completely open to question.").

decision could not agree on fundamental aspects of that ruling. When this lack of consensus over the meaning of *Katz* is combined with the emptiness of the legal norms that *Katz* announced, it is not surprising to find that *Katz* has been a poor guardian of Fourth Amendment rights.

III. WHAT IMPACT WILL *KYLLO* HAVE?

A. Kyllo's *Impact on Earlier Cases Limiting the Scope of the Fourth Amendment*

The above discussion described the similarities of *Katz* and *Kyllo*, and argued that *Katz* has been a weak protector of Fourth Amendment rights. *Kyllo*'s impact on search and seizure interests, of course, is uncertain at this point. I suspect, however, that *Kyllo*, like *Katz*, is unlikely to prevent the use of technology to monitor and reveal information helpful to law enforcement officials. One reason why *Kyllo*'s impact may be blunted is because the Court may be unwilling to follow the implications of *Kyllo*'s holding in future cases. Consider, for example, a couple of precedents that seem undermined by *Kyllo*'s logic.

When explaining why thermal imaging constituted a search, Justice Scalia seemed annoyed with Justice Stevens's numerous statements that thermal imaging did not reveal information regarding the interior of the home. In Scalia's view, "a thermal imager reveals the relative heat of various rooms in the home."[207] Although that information was not "particularly private or important," there was no basis for concluding it is not "information regarding the interior of the home."[208] Justice Scalia also curtly dismissed Justice Stevens's comparison of thermal imagining to what a passerby might be able to observe by using ordinary human senses.[209] Justice Scalia noted that the dissent's comparison was "quite

[207] Kyllo v. United States, 533 U.S. 27, 35, n.2 (2001).

[208] *Kyllo*, 533 U.S. at 35 n.2.

[209] According to Justice Stevens, "any member of the public might notice that one part of a house is warmer than another part or a nearby building if, for example, rainwater evaporates or snow melts at different rates across its surfaces." *Id.* at 43 (Stevens, J., dissenting). Justice Stevens's logic is reminiscent of Chief Justice Burger's analysis in *Ciraolo*. In *Ciraolo*, Chief Justice Burger concluded that police use of an airplane to observe the defendant's backyard curtilage was not a search because "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed." Ciraolo v. California, 476 U.S. 207, 213-14 (1985).

irrelevant" because "[t]he fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment."[210]

Justice Scalia's conclusion that thermal imaging is a search is more convincing than Justice Stevens's contrary judgment. But if Justice Scalia is correct to say that thermal imaging is a search because it reveals information regarding the interior of the home, why isn't a police pen register—which also reveals information regarding the interior of a home, to wit: the telephone numbers dialed-a search? As noted earlier, *Smith v. Maryland* held that a pen register was not a search.[211] One might try to distinguish *Smith* by arguing that a pen register does not involve a police intrusion *into* the home, but a thermal imager does not invade the home either. Both the government and Justice Stevens emphasized that because a thermal imager only detects heat that radiates from the external surface of a home, it did not trigger Fourth Amendment protection, a point that Justice Scalia did not contest.[212]

Alternatively, one might try to distinguish *Smith* by arguing that a homeowner assumes the risk that the police would learn the numbers he dialed from his home because those numbers were revealed to the telephone company, which, in turn, was free to provide the numbers to the police. Although the *Smith* Court accepted that rationale, it is not a

---

[210] *Kyllo*, 533 U.S. at 35, n.2. Interestingly, Justice Scalia's rebuttal to Justice Stevens's argument sounded more like Anthony Amsterdam than Warren Burger. In his seminal article on the Fourth Amendment, Professor Amsterdam explained why the availability of information from unofficial sources does not give the government *carte blanche* to utilize police methods to obtain that same information. *See* Amsterdam, *supra* note 23 at 406-07 ("Every person who parks his or her car on a side street in Greenwich Village voluntarily runs the risk that it will be burglarized—a risk, I should add as one who has lived in Greenwich Village, that is very much higher than the risk of betrayal by your friends even if you happen to choose your friends exclusively from a circle of Machiavellian monsters. Does that mean that government agents can break into your parked car uncontrolled by the fourth amendment? Or pay the junkies to break into it?").

[211] Smith v. Maryland, 442 U.S. 735, 741 (1979).

[212] *See Kyllo*, 533 U.S. at 41 (noting that the police observations "were made with a fairly primitive thermal imager that gathered data exposed on the outside of petitioner's home but did not invade any constitutionally protected interest in privacy") (Stevens, J., dissenting) (footnote omitted); *id*. at 44 ("equipment in this case did not penetrate the walls of petitioner's home, and while it did pick up `details of the home' that were exposed to the public, it did not obtain `any information regarding the *interior* of the home.'"); Brief for the United States at 19, *Kyllo* (No. 99-8508) ("the imager did not literally or figuratively penetrate the walls of petitioner's house and perceive private activities inside"); *id*. at 26 (stating that the thermal imager detected "only heat radiating from the external surface of the house").

convincing legal theory to measure the scope of the Fourth Amendment.[213] But even if one is persuaded by risk theory, that logic is equally applicable to Danny Kyllo's case. Indeed, the court of appeals, the Solicitor General's office, and Justice Stevens all endorsed the notion that Kyllo assumed the risk that someone located outside might detect the heat emanating from his home.[214] According to Justice Stevens, society is unlikely to suffer from "a rule requiring the rare homeowner who both intends to engage in uncommon activities that produce extraordinary amounts of heat, and wishes to conceal that production from outsiders, to make sure that the surrounding area is well insulated."[215]

Moreover there are additional similarities between a thermal imager and a pen register. In *Kyllo*, Justice Scalia explained that a search occurs whenever police use "sense-

[213] *See e.g.*, United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) (noting that the "risk analysis" model of prior cases "lead to the substitution of words for analysis. The analysis must, in my view, transcend the search for subjective expectations or legal attribution of assumptions of risk. Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present."); Slobogin, *supra* note 28, at 1417 (noting that assumption of risk theory is "vacuous" in *Kyllo*: "The most pertinent illustration of that fact is that until the Supreme Court decision in *Kyllo*, in most jurisdictions we `assumed the risk' that police subject the interior of our houses to thermal imaging without obtaining a warrant or developing any level of suspicion that evidence of a crime would be discovered."); *cf.* Amsterdam, *supra* note 23, at 470, n.492 ("The question is whether the [F]ourth [A]mendment regulates the activity of the police in dispatching spies to insinuate themselves into people's confidences and homes . . . . If it does not, then the government may unleash its spies on any of us, criminals or not; and talk about `criminals' assuming the risks means that we all assume the risks."); Baldwin v. United States 450 U.S. 1045 (1981) (Marshall, J., dissenting). In *Baldwin*, the Court denied certiorari to review the claim that a search occurred when an undercover agent, who had obtained a position as the defendant's handyman and chauffeur, obtained samples of cocaine from the defendant's home. *Baldwin*, 405 U.S. at 1045. Justice Marshall complained that under the logic of the lower court, "the Government need never satisfy the probable-cause and warrant requirements of the Fourth Amendment if, by disguising its officers as repairmen, babysitters, neighbors, maids, and the like, it is able to gain entry into an individual's home by ruse rather than force in order to conduct a search." *Id*. at 1049 (Marshall, J., dissenting) (footnote omitted).

[214] *See* United States v. Kyllo, 190 F. 3d 1041, 1046 (9th Cir. 1998) (explaining that Kyllo "took no affirmative action to conceal the waste heat emissions created by the heat lamps needed for a success indoor grow"); Brief for United States at 25, *Kyllo* (No. 99-8508) ("When a government investigator is in a public place and uses technology to observe an area exposed to the public; it does not constitute a search, provided that technology does not directly detect private activity (or other private details) occurring in a private area."); *Kyllo*, 533 U.S. at 45 (Stevens, J., dissenting).

[215] *Kyllo*, 533 U.S. at 45 (Stevens, J., dissenting).

enhancing technology [to obtain] any information regarding the interior of the home that could not otherwise have been obtained without physical `intrusion into a constitutionally protected area.'"[216] Under this standard, a pen register is also a search because it is technology that enables the police to obtain information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into the home. The pen register reveals the numbers dialed on a home telephone that would otherwise be unavailable unless officers were inside the home to observe the dialing.[217] Furthermore, a pen register is not a device generally used by the public.[218] And finally, the pen register reveals details about the home. Indeed, a pen register provides more revealing and intimate details about the home than a thermal imager. While a thermal imager measures relative amounts of heat that may be escaping the home, a pen register identifies the people and organizations called by a homeowner, and thus reveals "the most intimate details of a person's life."[219]

In sum, the legal analysis that dictates the conclusion that thermal imaging is a search also compels the conclusion that a pen register is a search. Despite the parallels between a thermal imager and a pen register, Justice Scalia made no effort to reconcile *Kyllo*'s holding with *Smith v. Maryland*.[220] This is not to suggest that the Justices comprising the *Kyllo* majority are ready to reconsider or overrule *Smith*. If forced to revisit the constitutionality of pen registers, it is highly

[216] *Id.* at 34 (citation omitted).

[217] Of course, one might argue that because the police could subpoena a person's telephone records and obtain information about the numbers dialed within a home, the Fourth Amendment does not bar the police from obtaining that same information pursuant to a pen register. Under *Kyllo*'s analysis, however, a pen register does not become a non-search simply because the information revealed by the pen register is available from other sources. *Id.* at 35, n.2 ("The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment.").

[218] *See* Carrie L. Groskopf, *If It Ain't Broke, Don't Fix It: The Supreme Court's Unnecessary Departure From Precedent in* Kyllo v. United States, 52 DEPAUL L. REV. 201, 243 (2002) ("A pen register, in fact, is a device geared specifically for law enforcement purposes, and not for individual use. It would seem then, that under the reasoning of *Kyllo*, because a pen register is arguably *not* considered to be commonly available to the general public, the employment of a pen register should be unconstitutional.") (footnote omitted).

[219] Smith v. Maryland, 442 U.S. 735, 748 (1979) (Stewart, J., dissenting).

[220] While Justice Scalia did not attempt to reconcile his logic with *Smith*'s holding, Justice Stevens argued that technological equipment that disclosed "only the relative volume of sound leaving [a telephone] booth, which presumably was discernible in the public domain," would be constitutional under *Smith*'s holding. *Kyllo*, 533 U.S. at 49-50, n.6 (Stevens, J., dissenting).

likely that the current Court would reaffirm *Smith*'s holding notwithstanding the result in *Kyllo*. That said, Justice Scalia's silence regarding *Smith* is worth mentioning. Notwithstanding the shared traits between a thermal imager and a pen register, Justice Scalia's analysis in *Kyllo* proceeds forward oblivious to the tension between *Kyllo*'s holding that thermal imaging is a search and *Smith*'s ruling that a pen register is not a search. Conceivably, Justice Scalia did not notice the tension between *Kyllo*'s holding and *Smith*'s holding, although that is an unlikely scenario since a number of law professors immediately recognized the tension.[221] Perhaps, Justice Scalia's silence was compelled by the need to maintain the vote of one or more members of the *Kyllo* majority who were unwilling to join an opinion that cast doubt on the result in *Smith*. Whatever the explanation, at some point in the future, the Court may be forced to address the conflict between *Kyllo* and *Smith*. When that happens, my prediction is that the Court will confine *Kyllo*'s reasoning to its special facts, reaffirm *Smith*'s holding, and find that the Fourth Amendment presents no obstacles to using technology that is the functional equivalent of a pen register.[222]

Another precedent that *Kyllo*'s reasoning undermines is

---

[221] *See e.g.*, Joshua Dressler, posting on Jan. 17, 2002 (copy on file with author) ("Of course, after *Kyllo* last year, one can seriously question whether *Smith v. Maryland* can be justified on any reasonable basis of principle. If a thermal imager used outside a house to detect heat levels inside a house is unconstitutional (in the absence of a warrant), one wonders why the rule should be different in the case of a pen register obtaining phone calling activities inside."). *But cf.* Norman M. Garland, posting on Jan. 17, 2002 (copy on file with author) ("I think that [*Kyllo*] reaffirms the validity of the *Smith* case. Scalia, for the majority, cites *Smith* to distinguish it from the case before it."). I think that Professor Garland places too much weight on Justice Scalia's citation of *Smith*. Justice Scalia's sole reference to *Smith* occurs in Part II of his opinion which describes the law concerning police activities that trigger Fourth Amendment protection. As Professor Garland notes, Justice Scalia states that the *Katz* test has been applied "in holding that it is not a search for the police to use a pen register at the phone company to determine what numbers were dialed in a private home, *Smith v. Maryland*, 442 U.S. 735, 743-744 (1979)." *Kyllo*, 533 U.S. at 33. Scalia then explains that *Kyllo* "involves officers on a public street engaged in more than naked-eye surveillance of a home," and comments that the Court has "previously reserved judgment as to how much technological enhancement of ordinary perception from such a vantage point, if any, is too much." *Id.* Justice Scalia's standard of review is announced in Part III of his opinion. S*ee Id.* at 34. After announcing that standard, Justice Scalia never compares or contrasts the holding in *Smith* with the standard established in *Kyllo*. Thus, rather than distinguish *Smith*'s holding from the rule announced in *Kyllo*, Justice Scalia is, at best, indifferent to *Smith*, and makes no effort to reconcile his own reasoning with *Smith*'s analysis and holding.

[222] *See infra* notes 343-59 and accompanying text.

United States v. Place.[223] *Place* permitted police use of another type of technology—albeit canine technology—that has impacted Fourth Amendment rights.[224] *Place* held that a canine sniff of luggage that discloses only the presence or absence of narcotics is not a search.[225] In his *Kyllo* dissent, Justice Stevens complained that the Court's rule would cover devices that are designed to detect emissions coming from a house.[226] Justice Stevens sensibly noted *Place*'s holding would authorize "sense-enhancing equipment that identifies nothing but illegal activity."[227] According to Justice Stevens, *Place*'s holding has been diluted because use of a mechanical dog or other type of technology directed at home that might detect "the odor of deadly bacteria or chemicals for making a new type of high explosive" would be illegal under *Kyllo*'s reasoning.[228]

Interestingly, Justice Scalia chose not to respond to Justice Stevens's comments on the future viability of *Place*'s holding concerning technological devices that provide information regarding the interior of a home. Justice Scalia's silence on this point is even more perplexing than his refusal to discuss *Kyllo*'s impact on *Smith*'s holding for two reasons. First, the conflict between *Kyllo* and extending *Place*'s holding to cover technological devices that reveal information about the inside of a home is even more striking than the tension between *Kyllo* and *Smith*. A dog sniff, whether mechanical or not, that detects the odor of contraband or deadly bacteria coming from a home is easily covered by *Kyllo*'s rule that a search occurs whenever "sense-enhancing technology [enables the police to obtain] any information regarding the interior of [a] home that could not otherwise have been obtained without physical `intrusion into [the home].'"[229] Second, when *Kyllo* was under review by the Court, an influential federal court of appeals had already ruled that

---

[223] 462 U.S. 696 (1983).

[224] *Place*, 462 U.S. at 707.

[225] *Id*. In a rather casual manner, and without prompting a dissent, *Place*'s holding was extended to automobiles in *Indianapolis v. Edmond*, 531 U.S. 32, 40 (2000). *Edmond* ruled that a narcotics vehicle checkpoint was an unreasonable seizure because its primary purpose was law enforcement related. *Edmond*, 531 U.S. at 48. As it did in *Place*, the *Edmond* Court reached out to decide the constitutionality of a narcotics dog sniff of an automobile, even though that issue was unrelated to the central issue before the Court. *Id*. at 40. Speaking for the majority, Justice O'Connor, relying exclusively on *Place*, ruled that a canine sniff of a car is not a search. *Id*.

[226] *Kyllo*, 533 U.S. at 47 (Stevens, J., dissenting).

[227] *Id*.

[228] *Id*. at 48.

[229] *Id*. at 34.

Place's holding should not be extended to private homes.[230] It would be surprising that the Court was unaware of this development when deciding *Kyllo*.[231]

Moreover, several lower court judges have acknowledged the conflict between *Kyllo* and *Place*.[232] Although the lower courts have reached different results on the constitutionality of canine sniffs in various contexts, several judges have commented that *Kyllo* "appears to run counter to the analytical basis of the `dog sniff' rule."[233] My emphasis on the tension between *Kyllo* and *Place* is not to predict that the *Kyllo* majority is poised to overrule or reconsider *Place*. Indeed, during the same Term that *Kyllo* was decided, the Court unanimously held in *Indianapolis v. Edmond*[234] that a dog sniff of an automobile was not a search, and cited *Place* as the controlling precedent. Of course, under the Court's precedents, cars and containers found therein are not entitled to the same privacy interests that are afforded to homes,[235] but luggage is normally entitled to more privacy than cars,[236] unless, of course, the luggage is found inside an automobile.[237]

---

[230] United States v. Thomas, 757 F.2d 1359 (2d Cir. 1985).

[231] Professor LaFave's treatise gives prominent attention to *Thomas*. *See* LAFAVE, *supra* note 21, § 2.2(f) at 459. LaFave also highlights that the validity of *Thomas*'s legal analysis was questioned in *United States v. Colyer*, 878 F.2d 469 (D.C. Cir. 1989), which ruled that a dog sniff of a roomette in a train was not a search. *See* LAFAVE, *supra* note 21, § 2.2(f) at 460.

[232] *See, e.g.* United States v. Richard, No. CRIM 01-20048-01, 2001 WL 1033421, at *6 n.4 (W.D. La., 2001); State v. Wiegand, 645 N.W. 2d 125, 130 (Minn. 2002); People v. Haley, 41 P.3d 666, 671 n.2 (Colo. 2001); State v. Bergmann, 633 N.W.2d 328, 334 (Iowa 2001); State v. Miller, 647 N.W.2d 348, 355 n.2 (Wis. App. 2002) (Dykman, J. concurring).

[233] *Richard*, 2001 WL 1033421, at *6 n.4. *See also Wiegand*, 645 N.W.2d at 138 (Page, J., concurring) ("I do not see a distinction between sense-enhancement-by-technology and sense-enhancement-by canine."); *Haley*, 41 P.3d at 671 n.2 ("In our view, the logic of [*Kyllo*'s] holding undercuts the prosecution's argument that dog sniffs of the outside of an automobile to detect the contents thereof do not fall within a reasonable expectation of privacy.").

[234] 531 U.S. 32, 40 (2000).

[235] *See* California v. Carney, 471 U.S. 386 (1985). Chief Justice Burger's opinion in *Carney* held that the "automobile exception"—which permits warrantless searches of cars provided there is probable cause—controlled the search of a motor-home that was found in a public parking lot. *Carney*, 471 U.S. at 390-94.

[236] *See* United States v. Chadwick, 433 U.S. 1 (1977). *Chadwick* held that a warrantless search of a footlocker was unconstitutional, even though there was probable cause to believe it contained contraband. *Chadwick*, 433 U.S. at 15-16. In an opinion by Chief Justice Burger, the Court pointedly rejected the government's argument that the automobile exception should equally apply to movable containers, and that the warrant requirement should be confined to searches of homes and other areas of "core" privacy interests. *Id.* at 11-13.

[237] A description of the intricacies and absurdities of the Court's automobile

My point is not to predict the demise of *Place*. Rather, my contention is that *Kyllo* undercuts the argument that a dog sniff of an apartment or a roomette on a train is not a search under the Fourth Amendment. Like a thermal imager, a canine sniff is a law enforcement device that allows the police to obtain information regarding the interior of a home or other protected area that could not otherwise have been obtained without a physical intrusion.[238] Of course, dogs, more so than pen registers, electronic beepers and airplanes are generally available to the public,[239] which may make *Kyllo*'s reasoning inapplicable to canine sniffs.[240] As others have

search doctrine is beyond the scope of this article. Cases such as *Wyoming v. Houghton*, 526 U.S. 295 (1999), *California v. Acevedo*, 500 U.S. 565 (1991), and *United States v. Ross*, 456 U.S. 798 (1982) are examples of the Court's most recent pronouncements in this area.

[238] *Cf.* Thomas K. Clancy, *Coping with Technological Change:* Kyllo *and the Proper Analytical Structure to Measure The Scope of Fourth Amendment Rights*, 72 MISS. L.J. 525, 557 (2002) (asserting that the "logic of [*Kyllo*'s] analysis surely must apply to all technological devices that detect information about the interior of the home"). At least one lower court has intimated that *Kyllo* does not affect canine sniffs because a dog sniff is not "technology" within the meaning of the *Kyllo*'s holding. *See Wiegand*, 645 N.W.2d at 130 n.3. In *Wiegand*, the Minnesota Supreme Court distinguished the facts involved there, namely, a dog sniff of a car, by stating: "We are not faced with the issue of a dog sniff around a *home*, nor are we faced with an investigative technique involving a piece of *technology* with the potential for dramatic technological advancements." *Id.*; *see also Haley*, 41 P.3d at 677-78 (Kourlis, J., dissenting) (rejecting the majority's argument that *Kyllo* undermines *Place*'s logic: "A dog sniff is not a technological advancement that invites the same sort of concern [present in *Kyllo*]."). That conclusion misses the point of *Kyllo*. Justice Scalia specifically noted that the Court had "reserved judgment as to how much technological enhancement of ordinary perception from [a public] vantage point, if any, is too much." Kyllo v. United States, 533 U.S. 27, 33 (2001). Canine sniffs undoubtedly *enhance* the ordinary sensory faculties of police officers. In fact, police "use of a dog is not a mere improvement of their sense of smell, as ordinary eye glasses improve vision, but is a significant enhancement accomplished by a different, and far superior, sensory instrument." United States v. Thomas, 757 F.2d 1359, 1367 (2d Cir. 1985). While it is imaginable that a police officer, using her ordinary senses, might be able to discern the same information that a thermal imager reveals, *see Kyllo*, 533 U.S. at 43 (Stevens, J., dissenting) ("[T]he ordinary use of the senses might enable a neighbor or passerby to notice the heat emanating from a building, particularly if it is vented, as was the case here."), the dog sniff does what no ordinary person can do. *See* Harris, *supra* note 119, at 24 n.137 ("Although both man and dog can smell, the dog's nose was not simply a way to enhance what the human at the end of the leash could do. Rather, the canine nose is so much better—more sensitive and more accurate—than its human counterpart that it simply could not be said to replace it.").

[239] At least one state supreme court justice, however, has stated that a contraband sniffing dog should not be considered technology in general public use. *See Wiegand*, 645 N.W.2d at 138 (Page, J., concurring specially) ("In this case, the sense-enhancing dog sniff, *not in general public use*, obtained information regarding the interior of the vehicle. . . . ") (emphasis added).

[240] Whether the "general public use" rule is part of *Kyllo*'s holding is uncertain. "It is worth noting that the *Kyllo* majority never firmly adopted the general public use doctrine. In a footnote, it stated that general public use `may' be a factor in the search analysis, and intimated it might `reexamine' this factor

already noted, however, whether a particular device is in general public use should have no impact on Fourth Amendment analysis.[241] House burglars are prevalent too, but because I run the risk that my home may be burglarized does not mean that a warrantless police invasion of my house is not a search. Likewise, if technology gives the government access that is the functional equivalent of physical presence in my home, the general availability of that technology should not make a difference when deciding whether the *government's* use of that technology constitutes a search. A dog sniff is a *search* because it provides the functional equivalent of actual presence in the area being targeted.

Sooner or later, the Court will have the opportunity to address the conflict between *Kyllo* and *Place*. When that occasion arises, my prediction is the Court will give *Kyllo* a narrow reading and extend *Place*'s holding to authorize dog sniffs of private residences.[242] If my guess is correct, a major

in the future." Slobogin, *supra* note 28, at 1432 n.179 (citing *Kyllo*, 533 U.S. at 39 n.6).

[241] Justice Stevens correctly asserted that a "general public use" rule is "perverse because it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment become more readily available." *Kyllo*, 533 U.S. at 47 (Stevens, J., dissenting). For a compelling critique of the "general public use" factor apparently established in *Kyllo*, *see* Slobogin, *supra* note 28. In a pre-*Kyllo* article, Professor David Harris also pointed out the flaws in having the scope of the Fourth Amendment turn on what technology is generally available to the public. Harris, *supra* note 119, at 23 (noting that the "type of technology the public can possess may change with surprising speed. Worse, the Court's reasoning implies that citizens somehow assume the risk of being observed by whatever technology the government can muster for its crime-fighting efforts.").

[242] The Court will probably distinguish *Kyllo* in this context by explaining that a dog sniff only detects "the presence or absence of narcotics, a contraband item. Thus, despite the fact that the sniff tells the authorities something about the contents of the [home], the information obtained is limited." *Place*, 462 U.S. at 707. In contrast, the information disclosed by a thermal imager is not limited to detecting contraband. A recent lower court holding supports my prediction. *See* Porter v. Texas, No. 14-01-0177-CR to 14-01-0179-CR, 2002 WL 31008148 (Tex. App. Sept. 5, 2002). *Porter* held that a dog sniff of a home is not a search. *Porter*, 2002 WL 31008148 at *3. The *Porter* court explained that a dog sniff only discloses whether or not contraband is present and that a person does not have a legitimate expectation of privacy in possessing contraband. *Id*. *See also*, George M. Dery III, *The Loss of Privacy Is Just a Heartbeat Away: An Exploration of Government Heartbeat Detection Technology and Its Impact on Fourth Amendment Protections*, 7 WM. & MARY BILL RTS. J. 401, 412-13 (1999) (noting that the rule emerging from *Place* and *Jacobsen* is that if officials utilize devices that are "so precise as to identify nothing but illegally-possessed items, then the surveillance did not constitute a search"); Simmons, *supra* note 120, at 1352, n.208 ("[S]ince the Court in *Jacobsen* essentially held that there is no legitimate privacy interest in possessing illegal substances, the Court could easily

element of *Kyllo*'s framework will be diluted and the Court will have, literally and figuratively, "opened the doors" of people's homes to various types of technological devices that can selectively identify emissions coming from a home.[243]

In sum, *Kyllo*'s impact on future Fourth Amendment doctrine may be limited because Justice Scalia's opinion conflicts with key aspects of search and seizure law that currently permit technological and other sense-enhancing instruments to be used to gather information about "the most intimate details of a person's life."[244] Unless the Court is prepared to overrule (or severely limit) cases like *Smith v. Maryland* and *United States v. Place* (and there is no hint in *Kyllo* that the Court is ready to do this), the "right" announced in *Kyllo* will most likely be confined to a privilege against the use of a thermal imager directed at one's home.[245]

harmonize the *Kyllo* test with the *Place* doctrine by confirming that *Kyllo* only applies to areas, activities and items in which an individual has a legitimate expectation of privacy. The specific language used in *Kyllo* already implies this, since it limits the test to `details of the home,' which clearly deserve constitutional protection."); *cf.* Michael Adler, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L. J. 1093, 1098 (1996) (considering the Fourth Amendment implications of a "perfect search"—a computer program that would scan a hard drive and "report only the presence or absence of an *exact* copy of a certain piece of illegal modified software," and would "ignore everything else on the disk, no matter how blatantly illegal—or sensationally intriguing—a human investigator might find that information.").

[243] *Cf. Kyllo*, 533 U.S. at 45 (Stevens, J., dissenting) ("[P]ublic officials should not have to avert their senses or their equipment from detecting emissions in the public domain such as excessive heat, traces of smoke, suspicious odors, odorless gases, airborne particulates, or radioactive emissions, any of which could identify hazards to the community.").

[244] Smith v. Maryland, 442 U.S. 735, 748 (1979) (Stewart, J., dissenting).

[245] A few lower courts have already hinted that Kyllo's holding does not extend to the use of a thermal imager to scan premises other than the home, such as commercial premises. *See* United States v. Elkins, 300 F.3d 638, 646 (6th Cir. 2002) ("While *Kyllo* broadly protects homes against warrantless thermal imaging, the case before us involves the use of a thermal image to scan the Elkinses' *commercial* buildings.") (emphasis added); State v. Mordowanec, 788 A.2d 54 (Conn. 2002) ("The *Kyllo* decision did not address the question of whether a search warrant would be required to conduct a thermal imaging scan of premises other than a home, such as a commercial property. The court emphasized, however, the heightened expectation of privacy in one's home and distinguished that heightened expectation from the lesser expectation of privacy in a commercial property."). Although these cases did not resolve the constitutional issue at stake, they surely indicate a reluctance to extend *Kyllo*'s reach beyond a private home.

B. Kyllo *and Bright-Line Rules*

The second reason to question *Kyllo*'s impact on future cases focuses not on technology or scientific innovation, but on old-fashion Fourth Amendment doctrine. As noted earlier, Justice Scalia's opinion stressed the importance of bright-line rules, which provide guidance to police officers and judges who must follow and apply the Court's search and seizure doctrine. According to Justice Scalia, a clear constitutional rule was vital in *Kyllo* because "the Fourth Amendment draws `a firm line at the entrance to the house.' That line, we think, must be not only firm but also bright—which requires clear specification of those methods of surveillance that require a warrant."[246] Justice Stevens' dissent ridiculed the quality and clarity of Justice Scalia's *per se* rule, describing it as both "far too broad" and "too narrow," depending on the context.[247] To the surprise of many Court-watchers, Justice Stevens preferred giving politicians "an unimpeded opportunity" to resolve future developments concerning technology and Fourth Amendment rights, "rather than to shackle them with prematurely devised constitutional restraints."[248]

The important point here is not deciding who makes the better argument on the need for bright-line rules in the context of thermal imaging, but rather that Justice Scalia's conclusion on the need for *per se* rules is not likely to change or effect future Fourth Amendment doctrine, no matter how persuasive his arguments may have been in *Kyllo*. The Court's zigzag approach on the appropriateness of bright-lines in search and seizure cases is notorious.[249] There is no neutral

---

[246] *Kyllo*, 533 U.S. at 40 (citation omitted).

[247] As noted above, *see supra* notes 226-28 and accompanying text, Justice Stevens asserted that *Kyllo*'s rule was too broad because it would "embrace potential mechanical substitutes for dogs trained to react when they sniff narcotics," which would undermine the result and reasoning in *Place*. *Kyllo*, 533 U.S. at 47 (Stevens, J., dissenting). Justice Stevens also contended that *Kyllo*'s rule was unnecessarily broad because it covers any information regarding the interior of a home. *Id*. "If it takes sensitive equipment to detect an odor that identifies criminal conduct and nothing else, the fact that the odor emanates from the interior of a home should not provide it with constitutional protection." *Id*. at 48. At the same time, Justice Stevens criticized *Kyllo*'s holding as being too narrow.

> Clearly, a rule that is designed to protect individuals from the overly intrusive use of sense-enhancing equipment should not be limited to a home. If such equipment did provide its user with the functional equivalent of access to a private place—such as, for example, the telephone booth involved in *Katz*, or an office building—then the rule should apply to such an area as well as to the home.

Id. at 48-49 (Stevens, J., dissenting).

[248] *Id*. at 51.

[249] *See generally*, Albert W. Alschuler, *Bright Line Fever and the Fourth Amendment*, 45 U. PITT. L. REV. 227 (1984); Wayne R. LaFave, *The Fourth Amendment In An Imperfect World: On Drawing "Bright Lines" and "Good*

principle explaining the Court's willingness to use (or not use) bright-line rules. "[B]right lines will be applied when the Court decides to apply them."[250] There is no reason to think that *Kyllo* will alter this situation. Justice Scalia's triumph in *Kyllo* in persuading a majority of his colleagues on the benefits of bright-line rules will likely be a temporary victory.

The Court's most recent cases demonstrate how unlikely it is that *Kyllo*'s preference for bright-line rules will have a lasting impact. In the same Term in which *Kyllo* adopted a *per se* rule for determining whether thermal imaging was a search, the Court adopted a balancing analysis rather than a *per se* rule in another case involving the scope of protection the Fourth Amendment provides for the home. Decided four months prior to *Kyllo*, *Illinois v. McArthur*[251] concerned whether police, who had probable cause that marijuana was in a home, could seize the home and prevent the homeowner from entering his premises unaccompanied by an officer for approximately two hours while a search warrant was being obtained.[252] The Court concluded that the seizure was lawful.[253]

Two police officers accompanied Charles McArthur's wife when she went to his trailer-home to remove her belongings.[254] When the wife and the officers arrived, McArthur was *inside* his home.[255] The officers remained outside while the wife retrieved her possessions.[256] After gathering her belongings, the wife informed the officers that McArthur had concealed "`some dope underneath the couch.'"[257] The officers then knocked on the door and requested permission to search the home.[258] McArthur denied the request while standing outside his trailer.[259] The officer in

---

Faith", 43 U. PITT. L. REV. 307 (1982); *cf.* Tracey Maclin, *The Fourth Amendment on the Freeway*, [hereinafter, *The Fourth Amendment on the Freeway*], 3 RUTGERS RACE & L. REV. 117, 151-57 (2001) (arguing that the Court has yet to articulate a principled rule for deciding when a bright-line rule controls a Fourth Amendment issue involving a traffic stop).

[250] Maclin, *The Fourth Amendment on the Freeway*, *supra* note 249, at 157.

[251] 531 U.S. 326 (2001).

[252] *McArthur*, 531 U.S. at 329.

[253] *Id.* at 331.

[254] *Id.* at 328.

[255] *Id.* at 328-29.

[256] *Id.* at 329.

[257] *Id.*

[258] *Id.*

[259] *Id.* The officer in charge could not "recall whether he told [McArthur] to come out of the trailer or if [McArthur] came out on his own." People v.

charge then told McArthur that he could not reenter his home without a police escort.[260] The second officer left the scene to obtain a search warrant.[261] Two hours later, authorized by a search warrant, the police searched McArthur's home and found a small amount of marijuana and drug paraphernalia under the sofa.[262]

McArthur was charged with two misdemeanor offenses.[263] The Illinois judiciary sustained his claim that the police seizure of his home violated the Fourth Amendment, but Justice Breyer's opinion reached a different conclusion.[264] According to Justice Breyer, the central requirement of the Fourth Amendment is "reasonableness."[265] He explained that the Court interprets reasonableness "as establishing rules and presumptions designed to control conduct of law enforcement officers that may significantly intrude upon privacy interests."[266] Sometimes reasonableness requires warrants, but not always. Considering the totality of the circumstances in *McArthur*, Justice Breyer would not say "that the warrantless seizure was *per se* unreasonable."[267] Rather than announcing a bright-line rule, *McArthur* "balance[d] the privacy-related and law enforcement related concerns to determine if the intrusion was reasonable."[268] Under a balancing formula, Justice Breyer concluded that the seizure was reasonable.[269]

Why does the Court adopt a bright-line rule in *Kyllo*, but

McArthur, 713 N.E.2d 93, 94 (Ill. App. 4 Dist. 1999), *reversed*, 531 U.S. 326 (2001). McArthur's presence *inside* his home was a critical factor in the lower court's decision to sustain McArthur's Fourth Amendment claim. *See McArthur*, 713 N.E.2d at 98. For a discussion of why this point was critical to the constitutional issue in *McArthur*, see Craig M. Bradley, Illinois v. McArthur: *Preserving Evidence Pending Search Warrants*, TRIAL, JUNE 2001, at 70; Tracey Maclin, *Let Sleeping Dogs Lie: Why The Supreme Court Should Leave Fourth Amendment History Unabridged*, 82 B.U. L. REV. 895, 934-35 (2002).

[260] *McArthur*, 531 U.S. at 329.

[261] *Id.*

[262] *Id.*

[263] *Id.* McArthur was charged with unlawfully possessing drug paraphernalia and marijuana (less than 2.5 grams).

[264] *Id.* at 329-31.

[265] *Id.* at 330.

[266] *Id.* at 330.

[267] *Id.* at 331. According to Justice Breyer, the facts involved "a plausible claim" of exigent circumstances. He also noted that the seizure was tailored to the police need, was limited in time and scope, and avoided "significant intrusion into the home itself." *Id.*

[268] *Id.* (citing Delaware v. Prouse, 440 U.S. 648 (1979) and United States v. Brignoni-Ponce, 442 U.S. 873 (1975) which were not "house" cases).

[269] *Id.* For a critique of *McArthur* and an explanation why *McArthur* failed to address the crucial issue confronting the Court, see Bradley, *supra* note 259, at 70 (arguing that "the issue here is not one of sealing unoccupied premises but of seizing an occupied dwelling and ejecting the occupant").

prefer a balancing test in *McArthur*, even though both cases concern the sanctity and security of a home? One might say that because *Kyllo* involved the "threshold" issue of whether a search occurred, a *per se* rule is necessary to provide guidance for police officers. If the challenged police conduct does not involve a "search" within the meaning of the Fourth Amendment, police officers need not worry about the "reasonableness" of their actions. They are free to proceed without obtaining a warrant, and they need not worry whether they have probable cause or reasonable suspicion of criminality to justify their intrusion. On the other hand, in *McArthur* there was no question that a seizure had occurred. Thus, the "threshold" issue of whether the police conduct triggered Fourth Amendment scrutiny was not on the table. The only question confronting the Court concerned the "reasonableness" of the seizure. Reasonableness generally—although not always—requires a consideration of the totality of the circumstances.

If this explanation accurately describes the Court's approach, then *Kyllo* and *McArthur*—rather than illustrate the Court's unprincipled approach toward bright-line rules—demonstrate a coherent theme. But the two most recent cases involving whether a police intrusion constitutes a search, *Minnesota v. Carter*[270] and *Bond v. United States*,[271] cast doubt on the validity of this explanation. An earlier discussion noted the differences between *Kyllo*, which adopted a bright-line rule, and *Minnesota v. Carter*, which eschewed a *per se* rule for determining whether guests or visitors will have an expectation of privacy in their host's home.[272] Although both *Carter* and *Kyllo* involved the threshold issue of whether a search occurred, the Court took divergent paths to resolve this issue.[273]

Carter is not the only recent case where the Rehnquist Court avoids bright-line rules for determining whether a search has occurred. *Bond v. United States*,[274] decided a year before *Kyllo*, concerned whether an officer's squeeze of luggage triggered Fourth Amendment protection.[275] Steven

[270] 525 U.S. 83 (1998).
[271] 529 U.S. 334 (2000).
[272] See *supra* notes 78-102 and accompanying text.
[273] *Compare Carter*, 525 U.S. at 91 *with Kyllo*, 533 U.S. at 40.
[274] 529 U.S. 334 (2000).
[275] *Bond*, 529 U.S. at 335.

Dewayne Bond was a passenger on an interstate bus that was stopped at a border patrol checkpoint in Texas. An immigration officer squeezed Bond's canvas bag that was in the overhead compartment. The officer felt a "brick-like" object inside. A search of the bag revealed a "brick" of methamphetamine. The issue before the Court was whether the officer's squeeze constituted a search.[276] Writing for a seven Justice majority, Chief Justice Rehnquist ruled that the squeeze was a search. First, the Chief Justice explained that the officer's motive for touching the bag was irrelevant to the constitutional issue.[277] He then explained that while a bus passenger may expect that others will handle his luggage, a passenger "does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner."[278] Because the officer's squeeze was probing rather than the equivalent of what a passenger might do to create more room in the overhead rack, the Chief Justice held that a search occurred.[279]

In sum, *Carter* and *Bond* demonstrate that the Rehnquist Court is not devoted to bright-line rules when determining the scope of the Fourth Amendment. Notwithstanding sensible arguments to the contrary,[280] the Court established a legal framework where the constitutional rights of house guests and interstate travelers will depend on a balancing process that will be initially conducted by police officers who may be disinclined to respect the Fourth Amendment rights of individuals. Unlike the *per se* rule announced in *Kyllo*, the totality tests of *Carter* and *Bond* afford scant guidance to officers interested in knowing whether their actions trigger constitutional safeguards. In sum, the reasoning and results in *Kyllo*, *Carter* and *Bond* illustrate that the Court has yet to articulate a coherent rationale for deciding when a bright-line rule will be used to resolve whether a police intrusion constitutes a search under the Fourth Amendment.

---

[276] *Id.* at 35-36.

[277] *See Id.* at 338 n.2 ("[T]he issue is not his state of mind, but the objective effect of his actions.").

[278] *Id.* at 338-39.

[279] *Id.* at 339.

[280] *See* Minnesota v. Carter, 525 U.S. 83, 106-09 (1998) (Ginsburg, J., dissenting) (explaining why social guests and visitors should be entitled to rely on the privacy of their host's home). In *Bond*, Justice Breyer contended that the reasoning in that case "will lead to a constitutional jurisprudence of `squeezes,' thereby complicating further already complex Fourth Amendment law, increasing the difficulty of deciding ordinary criminal matters, and hindering the administrative guidance (with its potential for control of unreasonable police practices) that a less complicated jurisprudence might provide." *Bond*, 529 U.S. at 342 (Breyer, J., dissenting).

Even if one believes that threshold cases justify the use of *per se* rules and cases resolving the "reasonableness" of a challenged search or seizure should be resolved under a balancing formula, this distinction does not account for the methodology utilized in *McArthur*. As noted above, the Court has afforded the home the most scrupulous protection under the Fourth Amendment.[281] To promote the home's security, the Court has essentially adopted a *per se* rule regarding police intrusions into the home: "[T]he Fourth Amendment has drawn a firm line at the entrance to the house. Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant."[282] Granted, the police action in *McArthur* did not involve a forcible search or entry into a home, but it did breach the security McArthur enjoyed in his home. McArthur was inside his home when the police knocked and requested permission to search inside. When McArthur denied permission, he was forcibly detained outside his home while a search warrant was obtained.[283] This action certainly implicated the Fourth Amendment's explicit guarantee of a right "to be secure" in one's home.[284] Also, the need for police action in *McArthur* was less urgent than the justification rejected in *Welsh v. Wisconsin*,[285] which held the gravity of an offense is an important factor to consider when deciding whether exigency exists to justify a warrantless arrest inside a home.[286]

---

[281] *See* notes 91-100 and accompany text.

[282] Payton v. New York, 445 U.S. 573, 590 (1980); *see also* Kirk v. Louisiana, 122 S. Ct. 2458, 2459 (2002) ("police officers need either a warrant or probable cause plus exigent circumstances in order to make a lawful entry into a home").

[283] Illinois v. McArthur, 531 U.S. 326, 329 (2001).

[284] Although there was no forcible *entry* of his home, McArthur's right to enjoy full possession of his home and right to be secure within his home was disturbed by the police action. *Cf.* Clancy, *supra* note 238, at 541 (explaining that "the essential attribute of the right to be secure is the *ability* of the individual to exclude the government from intruding. Thus, . . . as to a seizure of property, the individual may exercise the right to remain in possession . . . . This ability to exclude is so essential to the exercise of the right to be secure that is proper to say that it is the equivalent to the right—the right to be secure *is* the right to exclude."); Clancy, *supra* note 1, at 357 (same); Adler, *supra* note 242, at 1120 (asserting that "the Founders' ultimate desire was not that the government be reasonable but rather that the people be *secure* in their persons, houses, papers, and effects").

[285] 466 U.S. 740 (1984).

[286] *Welsh*, 466 U.S. at 753. The police arrested Welsh inside his home without a warrant after they developed probable cause that Welsh had been driving while intoxicated. The state argued that exigent circumstances justified the arrest because evidence of Welsh's blood-alcohol level might have dissipated while waiting for a warrant to be secured. *Id.* at 753. The *Welsh* Court,

Concededly, reasonable minds can differ over whether the Court correctly resolved the issue at stake in *McArthur*.[287] My concern here is not whether the Court correctly decided the merits in *McArthur*; instead, my focus is on the methodology that the Court used to resolve the merits. Police intrusions that affect the security and sanctity of the home have traditionally been resolved by bright-line rules.[288] *McArthur* bucks that trend, but its explanations for eschewing a bright-line rule are hardly satisfying.[289] On the other hand, *Kyllo*,

however, invalidated the arrest because the state classified the offense "as a noncriminal, civil forfeiture offense for which no imprisonment was possible." *Id*. at 754 (citation omitted). In fact, *Welsh* moves close to announcing a *per se* rule against warrantless entries for arrest in cases of minor crimes. *See id*. at 753 ("[W]e note that it is difficult to conceive of a warrantless home arrest that would not be unreasonable under the Fourth Amendment when the underlying offense is extremely minor."); *id*. ("[A]pplication of the exigent-circumstances exception in the context of a home entry should rarely be sanctioned when there is probable cause to believe that only a minor offense, such as the kind at issue in this case, has been committed.").

In *McArthur*, Justice Breyer distinguishes *Welsh* on two grounds. *McArthur*, 531 U.S. at 336. First, he states that McArthur was detained for a "`jailable'" offense, whereas *Welsh* involved a "`nonjailable'" offense. *Id*. Second, he notes that the seizure involved in *McArthur* "is considerably less intrusive" than a police entry into a home to affect a warrantless arrest. *Id*. On the issue of exigency, Justice Breyer states that the facts in *McArthur* involve "a plausible claim" of exigent circumstances. *Id*. at 331.

[287] Professor Bradley calls the issue at stake in *McArthur* a "festering issue: When may police act to preserve evidence pending the arrival of a search warrant when they fear that someone inside the building may destroy the evidence?" Bradley, *supra* note 259, at 73.

[288] Exceptions to this statement may be Maryland v. Buie, 494 U.S. 325 (1990) and Richards v. Wisconsin, 520 U.S. 385 (1997). *Buie* held that the police may, while effecting the arrest of a felon in his home pursuant to an arrest warrant, conduct a protective sweep of a home when they have reasonable suspicion that the premises harbor an individual posing a danger to the officers or others. *Buie*, 494 U.S. at 337. *Richards* ruled that an unannounced entry into a home is permissible where the police have reasonable suspicion that knocking and announcing their presence and purpose would threaten officer safety or risk the destruction of evidence. *Richards*, 520 U.S. at 395.

[289] *McArthur*, 531 U.S. at 336. Justice Breyer explains that under the circumstances, "we cannot say that the warrantless seizure was *per se* unreasonable." *Id*. at 331. He then proffers two reasons for this conclusion. First, the facts involved "a plausible claim of specially pressing or urgent law enforcement need, *i.e.*, `exigent circumstances.'" *Id*. Second, he notes that the seizure of McArthur "was tailored to that need, being limited in time and scope, and avoiding significant intrusion into the home itself." *Id*. Justice Breyer's first justification for the seizure—"a plausible claim" of exigency—"is a concept unknown in the Court's Fourth Amendment jurisprudence, and [he] made no effort to explain it." Maclin, *supra* note 259, at 935 n.182. Judges and police officers will undoubtedly have trouble determining the difference between exigent circumstances, which permits a warrantless entry of a home to effect an arrest or search, *see* Minnesota v. Olson, 495 U.S. 91, 101 (1990), and "a plausible claim" of exigency, which, after *McArthur* permits something less than a full-blown seizure of a home, and an implausible claim of exigency, which presumably would not have permitted the seizure upheld in *McArthur*. Justice Breyer's second justification for upholding the seizure—it was "both limited and tailored reasonably to secure law enforcement needs while protecting privacy

decided four months after *McArthur*, utilizes a bright-line rule to determine whether police conduct directed at a home implicates the Fourth Amendment.[290]

Kyllo's preference for drawing a firm and bright line at the entrance to the house is equally applicable in *McArthur*: Absent exigent circumstances, police officers should not be allowed to disturb an individual's right "to be secure" in his home without a warrant. Although both cases involve the sanctity and security of a private home, the choice to employ a *per se* rule in *Kyllo* and a balancing test in *McArthur*, is not explained by the Court nor deciphered by examining the Court's relevant precedents.

C. Kyllo*'s Emphasis on the Home*

The third and final reason to question *Kyllo*'s long-term impact for protecting Fourth Amendment rights, ironically, concerns *Kyllo*'s strongest feature: its emphasis on the home.[291] The driving force of Justice Scalia's opinion was that

interests"—typifies the fact-specific balancing often seen in Justice Breyer's search and seizure opinions. *See, e.g.*, Bd. of Ed. v. Earls, 122 S. Ct. 2559, 2569-71 (2002) (Breyer, J., concurring) (listing factors that make drug testing program valid); Wyoming v. Houghton 526 U.S. 295, 308 (1999) (Breyer, J., concurring) (distinguishing between searching a woman's purse found on the backseat of a car, and searching a purse "attached to her person"); Minnesota v. Carter, 525 U.S. 83, 103-05 (1998) (Breyer, J., concurring) (asserting that the record did not support the factual conclusions of the lower court's determination that an officer's conduct constituted a search). But this approach to Fourth Amendment issues has its own problems, as Justice Breyer knows. *See* Bond v. United States, 529 U.S. 334, 342 (2000) (Breyer, J., dissenting) (complaining that the Court's ruling on whether an officer's squeeze of luggage constitutes a search complicates "already complex Fourth Amendment law, [and] increas[es] the difficulty of deciding ordinary criminal matters, and hinder[s] the administrative guidance (with its potential for control of unreasonable police practices) that a less complicated jurisprudence might provide"); *see also*, Wayne R. LaFave, *"Case-By-Case Adjudication" versus "Standardized Procedures": The* Robinson *Dilemma*, 1974 SUP. CT. REV. 127, 141 ("A highly sophisticated set of rules, qualified by all sorts of ifs, ands, and buts and requiring the drawing of subtle nuances and hairline distinctions, may be the sort of heady stuff upon which the facile minds of lawyers and judges eagerly feed, but they may be `literally impossible of application by the officer in the field.'") (footnote omitted).

[290] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[291] In his article on *Kyllo*, Professor Seamon describes *Kyllo* as an important case and also highlights the Court's emphasis on the home. *See* Richard H. Seamon, Kyllo v. United States *And the Partial Ascendance of Justice Scalia's Fourth Amendment*, 79 WASH. U.L.Q. 1013 (2001). According to Professor Seamon, *Kyllo* is a significant ruling, in part, "because it reinforces the narrowing of the once broad warrant presumption in two ways. First, by departing from the reverse *Katz* test [the tendency by the Court to find that government conduct is not a search for Fourth Amendment purposes], *Kyllo*

a thermal imager discloses information regarding the interior of a home.[292] While Justice Scalia willingly conceded that the challenged intrusion in Kyllo's case involved an insignificant compromise of a homeowner's privacy,[293] that fact was unimportant. The trivial nature of the intrusion was irrelevant because—from the Founder's era to modern times—private homes have been protected against warrantless police searches. Thus, Scalia explained that the Court "must take the long view, from the original meaning of the Fourth Amendment forward."[294] This meant that a search warrant was required before police could utilize a thermal imager to determine the relative heat that was emanating from Kyllo's home.[295]

To a certain extent, *Kyllo*'s emphasis on the home is understandable. There are textual, historical and practical reasons why the Court's Fourth Amendment jurisprudence has afforded the home special protection. *Kyllo* continues this trend, notwithstanding the limited information that the thermal imaging revealed. Practically speaking, however, giving special protection to the home, but reduced or no protection to other areas, may be short-sighted, particularly if the Court is concerned about technological advances that

may block future resort to that test as a means of shoring up the illusion of a broad warrant presumption. Second, *Kyllo* articulates the new, narrow version of the presumption, under which the warrant requirement applies most stringently to searches of the home." *Id.* at 1029. Although Professor Seamon generally applauds the result in *Kyllo*, a student commentator calls *Kyllo* "a dangerous opinion" because Justice Scalia:

> has crafted an opinion that moves the Court even further in reverse, back toward a Fourth Amendment jurisprudence based on place. And the only place that Justice Scalia appears to believe that warrants full protection is the interior of the home. The test he develops for whether government use of a technology constitutes a search offers little to no protection to information generated by new technologies.

Andrew Riggs Dunlap, *Fixing the Fourth Amendment with Trade Secret Law: A Response to* Kyllo v. United States, 90 GEO. L.J. 2175, 2176 (2002). According to Dunlap, *Kyllo*'s "reasoning should produce alarm" because it embraces "a view of the Fourth Amendment that buckles and gives way once a citizen, or his or her information, passes outside the home." *Id.* at 2187, 2189-90. While I agree that in future cases the Court is likely to read *Kyllo*'s holding narrowly, there is noting in *Kyllo* itself that demands this narrow interpretation.

[292] *Kyllo*, 533 U.S. at 35 n.2 ("A thermal imager reveals the relative heat of various rooms in the home. The dissent may not find that information particularly private or important, but there is no basis for saying it is not information regarding the interior of the home.") (citations omitted).

[293] *Id.* at 40.

[294] *Id.*

[295] *Id.*; *see also* David O. Markus & Mona Markus, *The Heat is On: Thermal Imaging and the Fourth Amendment*, THE CHAMPION Dec., 1998, at 22-24 (pre-*Kyllo* article arguing that the use of thermal imaging requires a judicial warrant).

intrude upon privacy. As Justice Stevens suggested, if sense-enhancing technology gives the government "the functional equivalent of access to a private place," then the reach of the Fourth Amendment protective umbrella should not be confined to the home.[296] Although the facts in *Kyllo* did not require the Court to discuss how its analysis might affect other areas and places entitled to constitutional protection, *Kyllo*'s stress on the home may provide a distinguishing point in future cases where the Court has to judge the use of thermal imaging or similar sense-enhancing equipment directed at targets other than houses. If the Court's past precedents are predictive of future results, the odds are good that *Kyllo*'s protective reach will be confined to the home. Indeed, the facts and holding of *United States v. Karo*[297]—another case involving electronic surveillance—reveals the limits of a judicial analysis focused on the home and may provide the template for limiting *Kyllo*.

In *Karo*, federal drug agents learned that the defendants had ordered several gallons of ether in order to extract cocaine from clothing that had been imported into the country. The agents placed an electronic beeper in a can of ether that was sold to the defendants.[298] Over a four month period, using both visual and electronic surveillance, the agents tracked the beeper as it arrived and left several private homes and two commercial storage facilities. Finally, the agents obtained a search warrant for a private residence where the beeper-laden can was located. Inside that home, they found cocaine.[299] Two issues confronted the Court: First, whether installation and transfer of the beeper-laden can to a buyer unaware of the beeper's presence triggered Fourth Amendment protection.[300] Second, whether monitoring of the beeper was a search when it revealed information that could not have been obtained through visual surveillance.[301] On the

---

[296] *Kyllo*, 533 U.S. at 48 (Stevens, J., dissenting) (citation omitted).

[297] 468 U.S. 705 (1984).

[298] The agents received a warrant for the installation and transfer of the beeper-laden can, but that warrant was later invalidated for misleading statements in the affidavit. *Karo*, 468 U.S. at 719 n.5.

[299] *Id.* at 708-10.

[300] *Id.* at 712.

[301] *Id.* at 714. On the first issue, *Karo* ruled that installation and transfer of the beeper-laden can was neither a search nor seizure. *Id.* No search occurred because the transfer of an unmonitored beeper "conveyed no information at all. To be sure, it created a *potential* for an invasion of privacy, but we have never held that potential, as opposed to actual, invasions of privacy constitute searches.

second issue, *Karo* ruled that "monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence."[302]

Seven Justices in *Karo* agreed that monitoring a beeper in a private home constitutes a search.[303] The Court was split, however, over whether monitoring the beeper to determine that it was located somewhere in a storage facility constituted a search. Writing for the majority, Justice White explained that no search occurred because the beeper disclosed only that the can was "somewhere in the warehouse."[304] The monitoring did not "identify the specific locker" which contained the beeper-laden can.[305] Nor did the monitoring reveal anything about the "contents" of the locker the defendants had rented.[306] Justice Stevens, however, took issue with this conclusion. He noted the agents were unaware of the beeper's location after its initial entrance into a private home. "From that moment on it was concealed from view."[307] The

. . ." *Id.* at 712. No seizure occurred either: "Although the can may have contained an unknown and unwanted foreign object, it cannot be said that anyone's possessory interest was interfered with in a meaningful way." *Id.*

[302] *Id.* at 714. The Court explained that beeper monitoring reveals "that a particular article is actually located at a particular time" in a home. *Id.* at 715. "Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers' observations but also established that the article remains on the premises." *Id.* at 715.

[303] *Id.* at 721. Justice O'Connor, with Justice Rehnquist joining her, stated that "the mere presence of electronic equipment inside a home, transmitting information to governments agents outside, does not, in and of itself, infringe on legitimate expectations of privacy of all who have an expectation of privacy in the home itself." *Id.* at 722 (O'Connor, J., concurring). She relied on *White*, which permitted the use of information obtained from within a home by means of a microphone secreted on a government agent. *Id.* In O'Connor's view, the crucial question in *Karo* is the defendant's interest in the container in which the beeper is placed. *Id.* at 724. "When a closed container is moved by permission into a home, the homeowner and others with an expectation of privacy in the home itself surrender any expectation of privacy they might otherwise retain in the movements of the container-unless it is *their* container or under *their* dominion or control." *Id.* (footnote omitted). According to Justice O'Connor, the beeper "transmitted information about the *location*, not the contents, of the container . . . . By giving consent to another to move a closed container into and out of the home the homeowner has effectively surrendered his privacy insofar as the location of the container may be concerned, or so we should assume absent evidence to the contrary. In other words, one who lacks dominion and control over the object's location has no privacy interest invaded when that information is disclosed." *Id.* at 727.

[304] *Id.* at 720.

[305] *Id.*

[306] *Id.* After the beeper monitoring revealed that the can was located in the storage facility, the locker containing the beeper-laden can was "identified only when agents traversing the public parts of the facility found that the smell of ether was coming from a specific locker." *Id.* at 720-21.

[307] *Karo*, 468 U.S. at 735 (Stevens, J., dissenting).

agents discovered the beeper's location in the storage facility by electronic surveillance.[308] "Without the beeper, the agents would have never found the warehouse . . . ."[309] Thus, Stevens concluded that because the monitoring "enabled the agents to learn the location of personal property otherwise concealed from public view," it was a search.[310]

The contrasting opinions of Justices White and Stevens illustrate the limits of a judicial analysis that emphasizes the home. According to the *Karo* majority, police may use electronic beeper surveillance free of constitutional scrutiny provided the monitoring discloses only "the general vicinity, and not the precise private location, of the [beeper]."[311] Justice White's judgment that "general vicinity" monitoring is not a search might not bother an agoraphobe, but it is an odd way to construe the Fourth Amendment, which protects other places and effects beside houses. Justice White is understandably concerned that "[i]ndiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."[312] But does the exact same "[i]ndiscriminate monitoring of property that has been withdrawn from public view" not present a similar serious threat to privacy interests when that surveillance reveals that property is located at a commercial storage facility, college campus or hotel resort? The fact that the indiscriminate monitoring did not identify the specific locker containing the property is beside the point. "The property was concealed from public view; its location was a secret and hence by revealing its location the beeper infringed an expectation of privacy."[313] Under Justice White's view, police are free to install covert electronic tracking devices on any item available for commercial purchase, for example, a book, suitcase or rental car. If later monitoring reveals that the property is located at a certain hotel resort or on a particular college campus, no search occurs provided the monitoring does not identify the specific room in which a

[308] *Id.*
[309] *Id.* at 735 n.11.
[310] *Id.* at 734-35.
[311] Fishman, *supra* note 160, at 342.
[312] *Karo*, 468 U.S. at 716 (footnote omitted).
[313] *Id.* at 735, n.11 (Stevens, J., dissenting).

person is staying.[314]

It may be possible in future cases to distinguish the thermal imaging directed at a home from thermal imaging directed at an office or other business facility.[315] Similarly, the Court may treat thermal imaging or other scientific searches of vehicles differently from the search in *Kyllo*.[316] Automobiles

[314] *See* Fishman, *supra* note 160, at 345. Professor Fishman recognizes that under *Karo*'s logic,

> it would appear that so long as the monitoring does not disclose conclusively which of two or more private locations (houses, hotel rooms, lockers, automobile trunks, or whatever) contains the beepered object, monitoring the beeper does not constitute a search. Such a rule would significantly diminish the privacy-enhancing impact the Court's holding in *Karo* that private location monitoring constitutes a search.

Fishman, *supra* note 160 at 345 (footnotes omitted). Interestingly, Professor Fishman criticizes Justice Stevens' conclusion that a search occurred when the agents in *Karo* utilized monitoring to determine that the beeper-laden can was located somewhere in the storage facility. According to Professor Fishman, this view "sweeps too broadly." Fishman, *supra* note 160, at 342. Professor Fishman explains:

> Had the agents maintained visual surveillance of the first storage facility, they *could have* observed the suspects transfer the ether from the first to the second warehouse. Further, upon learning that the ether had been removed from the first facility, the agents *could* have interviewed personnel at every other storage facility in Albuquerque until, *with luck* they found the warehouse in question. Alternatively, *in theory*, an informer *might have* learned of the ether's new location and reported it to the authorities. Any of these techniques would have "enabled the agents to learn the location of property otherwise concealed from public view," yet none of them would have "infringed upon a privacy interest protected by the Fourth Amendment." Why should using a beeper, to determine only the general vicinity to which the ether had been moved, be regarded differently? Justice Stevens enunciates no persuasive reason.

Fishman, *supra* note 160, at 342-43 (emphasis added). Professor Fishman's criticism of Justice Stevens resembles the reasoning of *Knotts*. In *Knotts*, the Court concluded that because officers "*could have*" observed the defendant as he traveled across the highways of Minnesota and Wisconsin, the Fourth Amendment does not bar the use of electronic surveillance equipment to allow the police to do the same. United States v. Knotts, 460 U.S. 276, 285 (1983) (emphasis added). The problem with both *Knotts*'s reasoning and Professor Fishman's analysis is that they each prove too much. As noted earlier, *see* notes 164-74 and accompanying text, one can always imagine methods in which police are able to detect useful information.

[315] In recent years, the Court has authorized warrantless and suspicionless searches of business offices and other premises on the basis of grounds that would not allow searches of homes. *See, e.g.*, New York v. Burger, 482 U.S. 691 (1987) (upholding warrantless, suspicionless search of automobile junkyard business on "special needs" theory); O'Connor v. Ortega, 480 U.S. 709 (1987) (searching of government employee's office assessed under "special needs" model; validity of the search "should be judged by the standard of reasonableness under all the circumstances"); *but cf.* Marshall v. Barlow's Inc., 436 U.S. 307 (1978) (invalidating warrantless search of business).

[316] *See, e.g.*, Dery, *supra* note 242, at 403. Professor Dery describes the many uses of the Enclosed Space Detection System (ESDS).

> The ESDS, or heartbeat detector, is a surveillance tool designed to detect the presence of people `hiding in enclosed spaces of vehicles' by

are entitled to a lesser degree of privacy than that given to houses. Therefore, a thermal imaging "search" or similar intrusion directed at a vehicle might not trigger Fourth Amendment protection, even though the intrusion reveals information "that would previously have been unknowable without [a] physical intrusion."[317] By combining the Court's judgment that vehicles are afforded diminished privacy protection, *Karo*'s conclusion that general vicinity monitoring is not a search, and *Kyllo*'s emphasis on the home, an analytical framework emerges that permits the Court to find that thermal imaging of targets other than houses does not implicate the Fourth Amendment.

In sum, *Kyllo* is an important ruling that expands Fourth Amendment protection. But *Kyllo*'s impact on future cases involving the Fourth Amendment and technology, beyond its limited fact pattern, is uncertain. If *Karo*'s reasoning on general vicinity monitoring is followed in future cases, the holding of *Kyllo* is unlikely to prevent government officers from using sophisticated technology to monitor or reveal information that is otherwise not exposed to public view.

IV. CARNIVORE MEETS *KYLLO*

As noted above, *Kyllo*'s long-term impact on search and seizure doctrine is uncertain. On the one hand, *Kyllo* may provide significant protection against future technological intrusions. In addition to reaffirming the principle that Fourth Amendment protection does not require a physical

> identifying the presence of a `human ballistocardiogram.' With each beat of the human heart, a ballistocardiogram or a small mechanical shock wave propagates through the body. This shock wave, in turn, causes the entire vehicle holding the person to vibrate `at a frequency dissimilar from any other source.'

Dery, *supra* note 21, at 653 (footnotes omitted).

[317] Kyllo v. United States, 533 U.S. 27, 40 (2001). *Karo*'s holding does not resolve whether electronic detection of an item concealed inside a vehicle constitutes a search. Professor LaFave explains that there is some "uncertainty" about the scope of *Karo*'s reach. LAFAVE, *supra* note 21, at 653. (noting that the Court initially frames the issue in broad terms as to "whether the monitoring of a beeper [is a search] when it reveals information that could not have been obtained through visual surveillance," but later in its opinion narrowly frames the issue as to "whether the monitoring of a beeper in a *private residence*, a location not open to visual surveillance" is a search) (emphasis added). According to Professor LaFave, *Karo* could be read to mean that beeper surveillance that reveals that a container is concealed inside a vehicle or other private location still amounts to a search, even though the surveillance is not directed at a private residence. LAFAVE, *supra* note 21, at 653.

intrusion into the home—a rule often ignored in previous cases involving technological intrusions—*Kyllo* also rejected the claim that disclosure of intimate details was necessary before a government intrusion would be deemed a search.[318] After *Kyllo*, *all* details regarding the interior of the home are constitutionally protected "because the entire area is held safe from prying governmental eyes."[319]

On the other hand, *Kyllo*'s protective impact may be blunted in future cases. *Kyllo*'s logic undercuts the holding in *Smith v. Maryland* and suggests that a dog sniff of a home is a search notwithstanding the contrary implication coming from *Place*. In light of the tension between *Kyllo* and these cases and because the Court is unlikely to overrule *Smith* or limit the logic of *Place* to luggage and automobiles, *Kyllo*'s holding may be confined to thermal imaging intrusions. Moreover, there is nothing in the *Kyllo* opinion that commits the Court to using "bright line" rules in future cases involving technological intrusions affecting the home. Finally, because *Kyllo* emphasized the traditional protection afforded private homes, it will be easy to distinguish *Kyllo* where technological intrusions do not target houses. Logically, the rule announced in *Kyllo* should "protect individuals from the overly intrusive use of sense-enhancing equipment" in other areas entitled to constitutional protection.[320] Yet, if the analysis of *Karo*—which *Kyllo* cites approvingly—is followed in future cases, *Kyllo*'s holding will not cover sense-enhancing equipment that reveals private information in protected areas outside of houses.

A possible test of *Kyllo*'s strength (or weakness) may come soon. The Court has not addressed the constitutional status of e-mail communications, and lower court rulings on the subject are sparse.[321] Normally, the Court is reluctant to address an issue that has not been percolating in the lower courts.[322]

---

[318] *Kyllo*, 533 U.S. at 38.

[319] *Id.* at 37.

[320] *Id.* at 48 (Stevens, J., dissenting).

[321] *See* Peter J. Georgiton, *The FBI's Carnivore: How Federal Agents May Be Viewing Your Personal E-Mail and Why There Is Nothing You Can Do About It*, 62 OHIO ST. L.J. 1831, 1838 (2001) (noting that the Court has not determined whether there is a "reasonable expectation of privacy in our personal home e-mail accounts, and there is little case law directed to the issue as well").

[322] *See* SUP. CT. R. 10; ROBERT L. STERN ET AL., SUPREME COURT PRACTICE 228 n.18 (8th ed. 2002) ("In some cases the Justices may feel that the time is not ripe for the Court to resolve a conflict, preferring to await further litigation that might produce a consensus or a satisfactory majority view among the lower courts."); *id.* at 230 (quoting Gilliard v. Mississippi, 464 U.S. 867 (1983) (Marshall, J., dissenting from denial of certiorari)) (addressing "`those of my Colleagues who agree with me [on merits of issue] but believe that this Court should

However, the constitutional questions surrounding Carnivore, the Federal Bureau of Investigation's controversial Internet surveillance program, may require the Court to address the constitutional status of e-mail communications coming from a home computer. If such a case arises, the Court may be confronted with a conflict between *Kyllo*'s holding and the government's claim that certain applications of Carnivore do not constitute searches under the Fourth Amendment.[323]

The exact contours and capabilities of Carnivore are still subject to debate.[324] Briefly stated, Carnivore is a computer-based search program that allows the FBI to intercept electronic communications that travel on the internet.[325]

---

postpone consideration of the issue until more state supreme courts and federal circuits have experimented with substantive and procedural solutions to the problem'").

[323] *See Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the House Subcomm. on the Constitution, House Comm. on the Judiciary*, 106th Cong. (2000) [hereinafter House Hearing] (statement of Donald M. Kerr, Assistant Director, Federal Bureau of Investigation) ("We do, in fact, have legal authority to do what we are doing today, and I think it is because of the correct belief, from my perspective, that the addressing information on the Internet is, in fact, a useful and appropriate analog to the telephone number in the switch circuit world."); *The `Carnivore' Controversy: Electronic Surveillance and Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong. (2000) [hereinafter Senate Hearing] (statement of Kevin DiGregory, Deputy Associate Attorney General Department of Justice) ("We don't think that there should be a different standard for the interception of e-mails versus the interception of telephones—excuse me; I used the word "interception"—for a pen register or a trap and trace for e-mails as opposed to a pen register or trap and trace for telephones.").

[324] *See* Maricela Segura, Note, *Is Carnivore Devouring Your Privacy?*, 75 S. CAL. L. REV. 231, 233 (2001) (noting that even "after independent review of Carnivore, questions linger about the program's actual capabilities").

[325] For a comprehensive description of Carnivore, *see* ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, *Independent Review of the Carnivore System, Final Report* (Dec. 8, 2000, at vii, *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf ("Carnivore is a soft-ware based tool used to examine all Internet Protocol (IP) packets on an Ethernet and record only those packets or packet segments that meet very specific parameters.") [hereinafter IITRI REPORT]; *see also* Ku, *supra* note 1, at 1355 ("Like an information roadblock, [Carnivore] screens all traffic, but pulls over only the data packets it has been programmed to capture."); Trenton C. Haas, Note, *Carnivore and the Fourth Amendment*, 34 CONN. L. REV. 261, 271 (2001) ("Carnivore is an Internet surveillance system or diagnostic tool, which—when equipped with special filtering software—gathers informational packets traveling over a network."); Neil King Jr. and Ted Bridis, *FBI's Wiretaps To Scan E-Mail Spark Concern*, WALL ST. J., July 11, 2000, at A3 (describing Carnivore as "[e]ssentially a personal computer stuffed with specialized software, Carnivore represents a new twist in the federal government's fight to sustain its snooping powers in the Internet Age. [Carnivore] can scan millions of e-mails in a second. . ."); Ted Bridis and Neil King Jr., *Carnivore E-Mail Tool Won't Eat Up Privacy, Says FBI*, WALL ST. J., July 20, 2000, at A28 ("The system belongs to a class of tools

> [Carnivore] enables the FBI to conduct a one-way tap into an Ethernet stream—the flow of electronic impulses carrying communications through an internet connection. This method allows investigators to search out keywords, e-mail addresses or internet protocol ("IP") addresses—a series of numbers and letters that correlate to websites. Carnivore can conduct at least two types of searches. First, installed on an ISP's [internet service provider] network, Carnivore can monitor and record the full content of messages that a targeted user has sent in real-time. This real-time, full-content search is conducted under the same basic legal structure that is employed for telephone wiretaps. Second, Carnivore is reportedly able to acquire the address information for the origin and the destination of all communications to and from a particular ISP customer. This function provides the TO and

known as `packet filters' or `sniffers,' which look for parcels of data that travel across a network and compromise an e-mail or a visit to a Web site. Using a Windows screen, Carnivore also can be set to capture file downloads and chat-room conversations. It can grab e-mail from the most popular Web-based companies, including Yahoo! Inc. and Microsoft Corp.'s Hotmail. And once it is installed at an Internet service provider, the FBI can dial into Carnivore to make changes and monitor data that have been collected."). The IITRI's REPORT on Carnivore, which was intended to address the complaints of civil libertarians and computer privacy advocates, was criticized by another group of experts. *See* Haas, *supra* note at 276 (explaining that "a five member team of renowned researchers and academicians" selected by the chief scientist at the Justice Department "harshly criticized the IITRI's review for what they considered `continued' and `serious concerns relating to Carnivore's system.'") (footnotes omitted).

The following law review articles have assisted me in understanding how Carnivore works, and have helped to identify the federal statutes that control various applications of Carnivore to electronic communications. Anthony E. Orr, Note, *Marking Carnivore's Territory: Rethinking Pen Registers on the Internet*, 8 MICH. TELECOMM. & TECH. L. REV. 219 (2002); Peter J. Georgiton, Note, *The FBI's Carnivore: How Federal Agents May Be Viewing Your Personal E-Mail and Why There Is Nothing You Can Do About It*, 62 OHIO STATE L. J. 1831 (2001); Trenton C. Haas, *Carnivore and the Fourth Amendment*, 34 CONN. L. REV. 261 (2001); Manton M. Grier, Jr., *The Software Formerly Known As "Carnivore": When Does E-Mail Surveillance Encroach Upon a Reasonable Expectation of Privacy?*, 52 S.C. L. REV. 875 (2001); Frank J. Eichenlaub, *Carnivore: Taking a Bite Out of the Fourth Amendment*, 80 N.C. L. REV. 315 (2001); Maricela Segura, Note, *Is Carnivore Devouring Your Privacy?*, 75 S. CAL. L. REV. 231 (2001); Thomas R. McCarthy, *Don't Fear Carnivore: It Won't Devour Individual Privacy*, 66 MO. L. REV. 827 (2001); Peter J. Young, *The Case Against Carnivore: Preventing Law Enforcement from Devouring Privacy*, 35 IND. L. REV. 303 (2001); Sandy D. Hellums, *Bits and Bytes: The Carnivore Initiative and the Search and Seizure of Electronic Mail*, 10 WM. & MARY BILL RTS. J. 827 (2001); Matthew Mickle Werdegar, *Lost? The Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy*, 10 STAN. L. & POL'Y REV. 103 (1998); Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J. L. & TECH. 75 (1994) (pre-Carnivore article discussing the constitutional and statutory issues surrounding stored and transmitted computer data). For a comprehensive and insightful article on the interplay between Fourth Amendment protection and various statutes designed to protect informational privacy, see Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1803 (2002).

> FROM addresses on an e-mail and is viewed as the electronic equivalent of a telephone pen-register or trap and trace search.[326]

This final section will examine what impact *Kyllo*'s holding will have for the second type of intercept Carnivore performs—its "pen mode"[327] application. Specifically, has a search under the Fourth Amendment occurred when the FBI employs Carnivore to intercept and record the routing and addressing information of e-mails sent from home computers?

A. Is E-mail Addressing Information Comparable To Telephone Numbers?

Justice Department officials have told members of Congress that *Smith v. Maryland* authorizes federal agents to use Carnivore's pen mode application without triggering Fourth Amendment protections.[328] According to this

---

[326] Segura, *supra* note 325, at 234 (footnotes omitted). A "trap and trace" search occurs when an electronic device is installed to "capture[ ] the incoming electronic or other impulses which identify the originating number" of an instrument or device from which a wire or electronic communication was transmitted. 18 U.S.C. § 3127(4) (1994). As another commentator has noted, the FBI "describes Carnivore as something of a magic wand, which, when `waved' over large volumes of e-mail, can be used to identify and separate targeted e-mails from non-targeted messages without violating the rights of those who use e-mail for lawful purposes." Eichenlaub, *supra* note 325, at 317.

[327] Under the "pen mode" or pen register mode, Carnivore "can collect header information such as the `TO:' and `FROM:' addresses from e-mails and the IP addresses of computers in FTP [File Transfer Protocol] or HTTP [Hypertext Transfer Protocol] transactions." Orr, *supra* note 325, at 223 (footnote omitted); *see also,* Georgiton, *supra* note 325, at 1842 (noting that "Carnivore can be set to retrieve only information concerning where an outgoing e-mail was sent, where an incoming e-mail was sent from, and the e-mail address itself") (footnote omitted); IIITRI REPORT, *supra* note 325 at ix ("In pen mode, the operator can see the TO and FROM e-mail addresses and the IP addresses of computers involved in File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP) sessions.").

[328] *See House Hearing, supra* note 323 (statement of Kevin DiGregory, Deputy Associate Attorney General Department of Justice) (responding to a question from Representative Jerrold Nadler that this information could be obtained without probable cause, DiGregory stated: "That's correct, and I want to point out to you that the Supreme Court held in *Maryland v. Smith,* I believe in 1979, that there was no reasonable expectation of privacy in numbers dialed by a telephone because essentially, when someone turns over information to a third part like the telephone company, they should not have either a subjective or an objective reasonable expectation of privacy in that information"). In responding to a question from Senator Leahy, which essentially asked if the use of Carnivore crossed the lines established in *Smith v. Maryland,* Donald Kerr responded:

> [W]e believe that such URL information is essentially identical to a

interpretation, federal agents "use Carnivore to conduct pen register searches because they believe that the addresses found in the TO and FROM lines of an e-mail are the electronic equivalent of the numbers dialed on a telephone."[329] Under *Smith*'s reasoning, a telephone pen register is not a search because a pen register "do[es] not acquire the *contents* of communications"[330] and because a telephone user has no reasonable expectation of privacy in the numbers dialed. By using his telephone and voluntarily conveying numerical information to the telephone company, a homeowner "assume[s] the risk that the company would reveal to police the numbers he dialed."[331]

The Justice Department's view that *Smith* authorizes application of Carnivore's pen mode without implicating Fourth Amendment safeguards has not been fully tested in the federal courts.[332] As one commentator has noted, "[n]o court has taken the inferential step and applied the *Smith* rule regarding the apprehension of telephone numbers to the apprehension of e-mail addresses through electronic surveillance."[333] But this same writer also acknowledged that

> telephone number within a telephone networks that a criminal may dial. Thus, it is worth noting that a Carnivore-based pen register would provide the FBI with virtually the same information as a telephone pen register would, i.e., the telephone number dialed by the criminal subject reflecting that a communication to XYZ Corp. had occurred. No "content" information (substance, purport or meaning) is gleaned from either type of pen register as to the nature of the call.

Senate Hearing, *supra* note 323 (statement of Donald M. Kerr, Assistant Director, Federal Bureau of Investigation).

[329] Segura, *supra* note 325 at 262 (footnote omitted); *see also* Georgiton *supra* note 325 at 1842 ("The FBI contends that, consistent with *Smith*, they can retrieve [information concerning where an outgoing e-mail was sent, where an incoming e-mail was sent from, and the e-mail address itself] without need for a warrant.") (footnote omitted).

[330] Smith v. Maryland, 442 U.S. 735, 741 (1979).

[331] *Smith*, 442 U.S. at 744.

[332] *See generally* Haas, *supra* note 325, at 281-84 (summarizing federal appellate court rulings finding that persons were not entitled to Fourth Amendment protection when using internet systems privately maintained by their employer or where the government seized messages found on a chat room that was open to the public, and explaining that these rulings "are considerably different from a situation involving the use of Carnivore by the FBI to intercept Internet e-mail messages from one individual to another"). United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996), which one commentator described as "[t]he leading case addressing the issue of privacy in personal e-mail accounts," *see* Georgiton, *supra* note 325, at 1839, did not consider the status of e-mail addressing information.

[333] Georgiton, *supra* note 325, at 1843. *But cf.*, Haas, *supra* note 325, at 289 (describing an unreported and sealed ruling of a United States Magistrate which "concluded that the FBI's proposed activities to intercept e-mail information was the function equivalent of capturing telephone numbers with a pen register or trap and trace device") (footnote omitted).

federal judges have not been eager to include e-mail addressing information under the Fourth Amendment's protective scope. Federal judges "while not explicitly considering whether a person has a reasonable expectation of privacy in the addressing information for their e-mail, have been largely reluctant to consider anything beyond the content of electronic communications in their *Katz* (reasonable expectation of privacy) analysis."[334]

Although the lower federal courts have not yet endorsed the Justice Department's position that application of Carnivore's pen mode to e-mail messages sent by or to home computers is authorized by *Smith*, academic commentators have reached divergent conclusions on the constitutionality of Carnivore's pen mode intercept. As an initial matter, several writers have acknowledged the uncertainty of *Smith* as applied to e-mail addressing information. For example, one student commentator acknowledges that the "language of *Smith v. Maryland* makes it difficult to conclude definitively whether Internet users hold any reasonable expectation of privacy in e-mail addressing information."[335] Nevertheless,

[334] Georgiton, *supra* note 325, at 1843 (footnote omitted). Although reported rulings on the constitutional status of e-mail addressing information have been rare, federal courts have often rejected claims that e-mail users' subscriber information is entitled to Fourth Amendment protection. Subscriber information typically includes an internet user's name; billing address; home, work, and fax numbers; and other billing information that is given to an internet service provider. Several federal courts, relying on *Smith*, have ruled that this information is not entitled to Fourth Amendment protection because individuals have no legitimate privacy interest in the account/subscriber information given to the ISP to establish an e-mail account. *See, e.g.*, Guest v. Leis, 255 F. 3d 325, 336-37 (6th Cir. 2001); United States v. Hambrick, No. 99-4793, 2000 WL 1062039, at *11-12 (4th Cir. Aug. 3, 2000); United States v. Cox, 190 F. Supp. 2d 330, 333 (N.D. N.Y. 2002); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

[335] Orr, *supra* note 325, at 226; *see also* Haas, *supra* note 325, at 290 ("At the outset, this Comment sought to establish whether Carnivore violated the Constitution's Fourth Amendment. Yet, after analyzing the issue, a yes or no answer is simply not possible. The issue is far more complex."); Segura, *supra* note 325, at 258 (noting that "there remains a constitutional question as to whether there is an expectation of privacy in e-mail, or whether it is a transactional record in the hands of a third party"); Georgiton, *supra* note 325, at 1842 (noting that *Smith*'s holding "*suggests* that the FBI does not need a warrant in order to get the addressing information from someone's e-mail account") (emphasis added). *See also* ROSEN, *supra* note 178 at 70-78. Professor Rosen notes:

> Personal e-mail poses something of a constitutional puzzle: on the one hand, it sometimes originates from work, which is not a place that the Fourth Amendment reserves for special constitutional protection; on the other hand, it seems analytically similar to a private letter, which is one

this writer concludes that e-mail users do not have a constitutionally protected interest in e-mail addressing information. E-mail users have no subjective expectation of privacy because "they certainly know that addressing information is being `conveyed' to their ISP, if for no other reason than to route their messages to the proper destination."[336] Moreover, because e-mail messages are typically stored on an ISP's computer equipment both before and after the recipient receives the message, users "know ISP's possess `facilities for recording' e-mail addressing information."[337] This writer also contends that no objective expectation of privacy exists in e-mail addressing information because the assumption of risk rule of *Smith* covers such information. Just as a person assumes the risk that the phone company will reveal to the police the numbers he dialed from his home telephone, a computer user assumes a similar risk by voluntarily conveying e-mail addressing information to an internet service provider. "A Carnivore installation on the ISP network simply facilitates this `revelation' by the ISP."[338]

Other academic commentators have sought to distinguish *Smith* by arguing that disclosure of e-mail addressing information reveals more information than a telephone pen register. *Smith* emphasized the "limited capabilities" of a pen register,[339] which, unlike a wiretap, had no capacity to disclose the content of a caller's communications. Carnivore's pen mode, by contrast, can reveal more information than a traditional pen register.

> Carnivore can be set to gather lists of the individuals a computer user has sent e-mail to and received e-mail from, lists of the computers the user has transferred files with, and lists of computers/web-servers accessed by the user in the

---

of the `papers' at the historical core of the Fourth Amendment.

Id. at 70.

[336] Orr, *supra* note 325, at 227.

[337] Orr, *supra* note 325, at 227, quoting Smith v. Maryland, 442 U.S. 735, 743 (1979).

[338] Orr, *supra* note 325, at 229. Another commentator has analogized e-mail addressing information to a traditional mail cover, which is not a search under the Fourth Amendment. Megan Connor Berton, *Home Is Where Your Modem Is: An Appropriate Application of Search and Seizure Law to Electronic Mail*, 34 AM. CRIM. L. REV. 163, 191-92 (1996) ("Just as senders of first class mail have little expectation of privacy in the information written or displayed on the outside of an envelope, e-mail users have little expectation of privacy in the address portion of their communications. This information is needed to deliver the message and, though often done solely by computer and without exposure to a human eye other than the recipient's, it is understood that any problems with the address causing difficulty in delivery may be noted by the system operator.").

[339] *Smith*, 442 U.S. at 742.

> course of surfing the Internet. These types of addressing information reveal much more than a telephone number does.[340]

Similarly, some legal commentators have also rejected the argument that e-mail addressing information is not entitled to constitutional protection because e-mail users knowingly convey that information to a third party. They argue that *Smith*'s assumption of risk rule should not apply to electronic communications because ISP employees sign employment agreements promising not to read or disclose private e-mail, and federal law does not authorize such disclosure.[341] Under this view, e-mail users "should have an [objective] expectation of privacy in their electronic communication, even if saved on a remote server."[342]

Given the logic of *Smith*, the Court is unlikely to recognize a constitutional difference between e-mail addressing information and the information that a telephone pen register reveals. Like a traditional pen register,

---

[340] Georgiton, *supra* note 325, at 1845-46; *see also* Segura, *supra* note 325, at 252 (arguing that the rationale supporting *Smith* is inapplicable in the electronic context "because e-mail addresses often do reveal the individuals involved in the communication, whether the address is a derivation of the individual's name, or the full name in parenthesis after the address"); Segura, *supra* note 325, at 262 (noting that "e-mail addresses often reveal the parties who are writing one other, and there is usually no question about whether the message was completed, as it is instantaneously sent to an internet mailbox") (footnote omitted); Chris J. Katopis, "*Searching*" *Cyberspace: The Fourth Amendment and Electronic Mail*, 14 TEMP. ENVTL. L & TECH. J. 175, 199 (1995) (arguing that "where a pen register and trap and trace device only reveal a telephone number, clearly much more information is obtained by analyzing the header of e-mail. The header is a portion of the transmission that does contain content"); *cf.*, Orr, *supra* note 325, at 231 (conceding that "it appears e-mail addressing information often does reveal more about the identity of the sender and receiver than the ten simple digits of a telephone number," but concluding "it is *unclear* whether e-mail addresses really reveal that much more about the identity of message senders and recipients") (emphasis added); Skok, *supra* note 25, at 75-79 (arguing that, although Web users reveal clickstream data to third parties, *Smith*'s assumption of risk theory should not apply to clickstream data because the clickstream reveals "a record of a person's cyberspace activity, [which] allows officers to entirely recreate an online experience").

[341] *See* Segura, *supra* note 325, at 253; *cf.*, 1 LAFAVE, *supra* note 21, § 2.6 at 120 (noting arguments that "`computer operators have no legitimate purpose in reading records unrelated to the operator's function, just as the telephone company has no legitimate purpose in listening to the contents of conversations,' and thus the user *does* have a legitimate expectation of privacy as to `the contents of electronic mail messages or personal files.' This is so even when the system manager makes backup copies of such records, and even when the users are all employees of the system operator.") (footnotes omitted).

[342] Segura, *supra* note 325, at 253.

Carnivore's pen mode does not disclose the content of e-mail messages.[343] To be sure, Carnivore's pen mode "does reveal more about the identity of the sender and receiver than the ten simple digits of a telephone number."[344] But the revelation of this additional information is probably not enough to persuade the Court that *Smith*'s reasoning should be

[343] Carnivore's pen mode collects "not only the `To:' and `From:' fields of targeted e-mail messages, but also the length of the message and the length of individual fields within those message. In fact, the system captures the entire e-mail message and all of its fields (including the `SUBJECT' line contents of the message), but replaces each character in fields other than `To:' and `From:' with an X." Orr, *supra* note 325, at 230. Many writers have asserted that Carnivore's pen mode reveals more information than a pen register, which thereby distinguishes the analysis of *Smith*. *See, e.g.*, Segura, *supra* note 325, at 262 ("As a basic matter, e-mail addresses often reveal the parties who are writing one other, and there is usually no question about whether the message was completed, as it is instantaneously sent to an internet mailbox") (footnote omitted); Georgiton, *supra* note 325, at 1845-46 (same); Haas, *supra* note 325, at 288 (same). For example, Carnivore can reveal the *length* of an e-mail message, which discloses more information than a pen register reveals. *See, e.g.*, Orr, *supra* note 325, at 230; Eichenlaub, *supra* note 325, at 330, n.105. This fact probably will not matter to the Court. Disclosure of the *length* of an e-mail message without revealing the *contents* of that message can be analogized to FBI agents learning the *length* of a telephone conversation without learning about the *contents* of the oral communications. If the pen register in *Smith* had disclosed the length of the calls along with the numbers dialed, I doubt that this additional information would have changed the result in that case. *See Smith*, 442 U.S. at 742 (noting that subscribers realize "the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills"). Most telephone bills also provide the length of long distance calls. Therefore, the fact that Carnivore's pen mode reveals the length of an e-mail message without disclosing its contents is unlikely to affect the Court's determination of whether a search has occurred. One commentator who argues that e-mail addressing information is not entitled to constitutional protection, nevertheless disagrees with my assessment that Carnivore's capability to record the length of an e-mail message will not affect the Court's judgment on the constitutional status of e-mail addressing information. *See* Orr, *supra* note 325, at 231-32. This commentator asserts that the problem of overcollection "may be a fatal constitutional flaw" because, unlike telephone numbers and e-mail addressing information, "the length of messages and the length of individual fields within those messages is not regularly collected for any legitimate business purpose." Moreover, Carnivore's "collection of the entire body of the message in "X" form" creates the potential for abuse because "if the software can electronically `redact' a message, perhaps it could also un-redact it, revealing the full contents." Accordingly, this writer concludes that Carnivore, as presently programmed, "should not be authorized for use as an Internet pen register." Orr, *supra* note 325, at 231-32.

While I agree that Carnivore's ability to capture the entire body of an e-mail message creates the potential for abuse, that fact will not make a difference to the Court. Long ago, the Court made clear technological devices that present a risk for invasions of privacy do not, standing alone, trigger Fourth Amendment protection. United States v. Karo, 468 U.S. 705, 712 (1984) (explaining that the installation of an unmonitored beeper "created a *potential* for an invasion of privacy, but we have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment . . . . It is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence.").

[344] Orr, *supra* note 325, at 231.

abandoned when deciding whether Carnivore's pen mode intercept constitutes a search. Similar arguments were raised in *Smith* to no avail. For example, Justice Stewart's dissent noted that telephone numbers dialed from a private line "are not without `content.'"[345] A pen register discloses to government officials "the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[346] In like manner, Justice Marshall's dissent contended that giving police officials unfettered discretion to employ pen registers jeopardized privacy, as well as First Amendment, interests.

> The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of personal contacts. Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society.[347]

These arguments did not convince the *Smith* majority that a pen register invades a homeowner's privacy when he uses a telephone,[348] and there is no reason to think that similar arguments will persuade the Court to discard *Smith*'s reasoning when determining Carnivore's pen mode intercept constitutes a search.

Likewise, the Court is unlikely to abandon the assumption of risk rule when it confronts the constitutional status of e-mail addressing information. *Smith* concluded that when a homeowner voluntarily conveyed numerical information to a third party, he "assumed the risk" that the third party would reveal that information to the government. As one commentator has recognized, *Smith*'s logic is equally

---

[345] *Smith*, 442 U.S. at 748 (Stewart, J., dissenting).

[346] *Id.*

[347] *Id.* at 751 (Marshall, J., dissenting) (citations omitted); *see also*, David E. Steinberg, *Making Sense of Sense-Enhanced Searches*, 74 MINN. L. REV. 563, 577 (1990) ("The pen register, however, cannot be limited to provide information only about phone numbers that may relate to criminal activity. Police will learn of all calls dialed by the suspect, and thus will discover if the suspect has talked to the girl next door, the local Alcoholics Anonymous hotline, or the national Communist Party headquarters.").

[348] *See* Werdegar, *supra* note 256, at 108 (1998)

applicable to e-mail addressing information.[349] It will not matter that ISP employees "must sign a confidentiality agreement that they will not read [or disclose] customer communications such as e-mail."[350] Telephone operators presumably operated under similar restraints when *Smith* was decided, and even if such restraints did not exist, the employment policies and practices of telephone companies were irrelevant to the result in *Smith*.[351] What was relevant in *Smith*, and will be relevant in a future case involving e-mail addressing information, is the homeowner's voluntary decision to convey information to a third party. Under the assumption of risk theory, the disclosure of information to a third party denies Fourth Amendment protection to what might otherwise be private information.[352]

In sum, if the analysis of *Smith* determines the constitutional status of e-mail addressing information, then Carnivore's pen mode intercept will not be considered a search under the Fourth Amendment. The two main features that compelled the Court to find that a pen register was not a search—the non-disclosure of the contents of communications and the fact that the individual assumed the risk that private

---

[349] Orr, *supra* note 325, at 229 ("Substituting the proper e-mail terms into [*Smith*'s] formula, it becomes clear that e-mail addressing information revealed to no one other than an ISP's equipment nevertheless falls squarely within the *Miller* assumption of risk doctrine, as interpreted in *Smith*."); Ku, *supra* note 1, at 1356 ("If Carnivore is programmed, for example, to capture the addresses of people with whom an individual is corresponding via e-mail, the analogy to *Smith* and the capturing of telephone numbers is even closer.").

[350] Segura, *supra* note 325, at 253.

[351] In *Smith*, the defendant argued that he had an expectation of privacy in the local calls he dialed because telephone companies typically do not record local calls. The Court concluded that argument lacked any merit:

> The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not, in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record. In these circumstances, petitioner assumed the risk that the information would be divulged to police. Under petitioner's theory, Fourth Amendment protection would exist, or not, depending on how the telephone company chose to define local-dialing zones, and depending on how it chose to bill its customers for local calls . . . . We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation.

Smith, 442 U.S. at 745.

[352] *See* Orr, *supra* note 325, at 229 ("When an Internet user sends a message over an ISP's network, she has revealed the addressing information to the ISP's equipment in the ordinary course of business, and she assumes the risk that the ISP will reveal her addressing information to the government. A Carnivore installation on the ISP network simply facilitates this `revelation' by the ISP.") (footnote omitted).

information would be revealed to the government—apply equally to e-mail addressing information. Thus, if *Smith*'s holding is the Court's "last word" on this issue, the Justice Department correctly concludes that the FBI is free to use Carnivore's pen mode intercept without triggering Fourth Amendment scrutiny.

B. Does Kyllo*'s Holding Cover E-Mail Addressing Information?*

Smith's holding, however, is not the end of the line. The rule established in *Kyllo* is pertinent to the constitutional status of e-mail addressing information. *Kyllo* holds that a search occurs when government actors acquire by "sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical `intrusion into a constitutionally protected area.'"[353] If this standard is applied to Carnivore's pen mode, then intercepting e-mail addressing constitutes a search.

Carnivore's pen mode enables the FBI to obtain by technology information regarding the interior of the home that could not otherwise be obtained without physical intrusion into a home. A pen mode intercept allows FBI agents to monitor information regarding the recipients and senders of e-mail messages sent from or to a homeowner's computer. This information would be unavailable to the government unless FBI agents were inside the home and had access to a computer user's e-mail account. Moreover, it is obvious that Carnivore is not a device generally available to the public and that Carnivore's pen mode provides greater detail about the inside of a home than a thermal imager, which only reveals the relative amount of heat escaping from a house. Finally, Carnivore cannot escape constitutional scrutiny because e-mail addressing information is available from a third party. Under *Kyllo*'s analysis, Carnivore does not become a non-search merely because the information acquired by a pen mode intercept is obtainable from an internet service provider.[354]

In sum, a straightforward application of *Kyllo*'s holding

[353] Kyllo v. United States, 533 U.S. 27, 34 (2001).

[354] *Kyllo*, 533 U.S. at 35, n.2 ("The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment.").

demonstrates that a search occurs when the FBI employs Carnivore to intercept and record the routing and addressing information of e-mails sent from or to home computers. If the Court is forced to address the constitutional status of e-mail addressing information, at least two options will be available. The Court can overrule *Smith v. Maryland* or confine *Kyllo*'s holding to thermal imaging. The likelihood that *Smith* will be overruled seems remote, although *Kyllo* substantially undermines *Smith*'s legal foundation. As noted above, the analytical framework that dictates the conclusion that thermal imaging is a search also compels the judgment that a pen register is a search.

On the other hand, limiting *Kyllo* to the narrow context of thermal imaging and not applying its holding to Carnivore is both unprincipled and perverse. A principled application of *Kyllo* would extend to its holding to all places and contexts entitled to Fourth Amendment protection.[355] Furthermore, Fourth Amendment law would be bizarre if *Kyllo* did not apply to Carnivore's pen mode. After all, the *Kyllo* majority was concerned about interpretations of the Fourth Amendment that would "leave the homeowner at the mercy of advancing technology."[356] Even commentators who believe that Carnivore can be re-programmed to comply with Fourth Amendment safeguards, concede that Carnivore, as currently programmed, reveals more private information than previously permitted under the Court's precedents.[357] It would be strange indeed for the Court to reject a "mechanical interpretation of the Fourth Amendment" when considering the constitutional status of a crude device that involves "no `significant' compromise of [a] homeowner's privacy,"[358] but then put aside its concerns about "advancing technology" and the privacy of the home when determining whether Carnivore's pen mode constitutes a search.[359]

What will the Court do? I predict that the Court will

---

[355] *See id*. at 48-49 (Stevens, J., dissenting).

[356] *Id*. at 35-36.

[357] *See, e.g.*, Orr, *supra* note 325, at 231.

[358] *Kyllo*, 533 U.S at 35 & 40.

[359] The invasiveness of Carnivore's reach has been described elsewhere. *See, e.g.*, Bridis & King, *supra* note 325, at A3 (quoting a former prosecutor saying that Carnivore is "the electronic equivalent of listening to everybody's phone calls to see if it's the call you should be monitoring. You develop a tremendous amount of information."); Haas, *supra* note 325, at 271 (attributing to Richard Forno the argument that "Carnivore is an electronic eavesdropping device"); Segura, *supra* note 325, at 231-32 (noting Carnivore "can conduct a far-reaching, general search of people who are not subject to a court order," and that many worry that "the Carnivore system will facilitate a `fishing expedition' in search of any evidence of crime").

conclude that Carnivore's pen mode does not violate the Fourth Amendment. The Court can achieve this result by using one of two modes of analysis. Under the first approach, as suggested, the Court will confine *Kyllo* to the context of thermal imaging and apply the analytical framework of *Smith* to conclude e-mail addressing information is not protected under the Fourth Amendment. If the Court adopts this model, *Kyllo*, like *Katz*, will become a "paper tiger" and will have little impact on the government's authority to use technology to gather information or monitor individuals' online activity.[360]

Under the second approach, the Court can avoid the tension between *Kyllo* and *Smith* by relying on its "special needs" cases to find that Carnivore's pen mode does not violate the Fourth Amendment. "Special needs" analysis is a fancy way to describe the balancing test performed by the Court in cases where the government lacks judicial authority or probable cause to conduct searches and seizures.[361] Indeed,

---

[360] *See* Skok, *supra* note 25, at 78-79, which argues that if *Smith*'s analysis is applied to clickstream data, then law enforcement officers will be able to know:

> not only what sites [an individual] visited, but also for how long each was visited, how often each site was re-visited, and which links were followed from each site. A comparable level of knowledge in the concrete world would require that the officers know not only which books the suspect borrowed, but also when she read the books, how long she spent reading each book and each page, and the sequence in which she read each book and each page.

Skok, *supra* note 25, at 78-79.

[361] At its inception, the "special needs" rule was intended as a narrow exception to the warrant and probable cause requirements. "Only in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable, is a court entitled to substitute its balancing of interests for that of the Framers." New Jersey v. T.L.O. 469 U.S. 325, 351 (1985) (Blackmun, J., concurring). Although intended as a limited exception, the special needs cases have expanded to the point where government actors are now permitted to conduct suspicionless searches in various contexts (including scenarios that involve criminal law enforcement) without establishing a compelling government interest. *See* JOSHUA DRESSLER, UNDERSTANDING CRIMINAL PROCEDURE 338-353 (3d ed. 2002). Professor Dressler explains that "when the Court determines that `special needs' exist, it evaluates the government activity—the special need—by [a] `reasonableness' balancing standard." *Id.* at 339. Not surprisingly, "nearly always, the government interest `trumps' the requirements of a warrant and/or probable cause (or reasonable suspicion)." *Id.* (footnote omitted). On the Constitution's 200th anniversary, Professor Kamisar explained why the "special" needs doctrine undermines core Fourth Amendment values:

> The handiness of the administrative search concept has gladdened the hearts of many government lawyers. But it has alarmed other observers, including me. Today, potential administrative searches are

"special needs" analysis may be an enticing framework to determine the constitutional status of e-mail addressing information because the Court has already used this doctrine to assess the constitutionality of drug testing programs in various contexts. Urinalysis, of course, is another type of technology that reveals information to the government that would otherwise be unavailable without the use of intrusive means by government officers.

Since 1989, the Court has decided six cases challenging the constitutionality of drug testing policies.[362] In only two cases, has the Court invalidated the urinalysis programs on Fourth Amendment grounds.[363] The three main factors considered by the Court in determining the validity of a drug testing regime are the nature of the privacy interest, the character of the intrusion, and the nature and immediacy of the governmental interests.[364] Applying this framework, the Court could decide that Carnivore's pen mode intercept constitutes a search, but the intrusion is conducted in a minimal manner and the government's need for e-mail addressing information "is important—indeed, perhaps

> buzzing around the Fourth Amendment like a swarm of bees. With drug and AIDS testing, the drone may soon grow deafening . . . . However great the threat posed by illicit drug use and the AIDS virus, the `individualized suspicion' concept must remain the heart of the Fourth Amendment. I believe we should greet claims of `national interest,' `emergency' or `necessity' with considerable skepticism. Slogans like these can be—and have been—a free people's most effective tranquilizers. As we mark the Constitution's 200th anniversary, we would do well to remember that.

Yale Kamisar, *Drugs, AIDS and the Threat to Privacy*, N.Y. TIMES, Sept. 13, 1987, § 6 (Magazine), at 109. For more recent academic commentary on the "special needs" cases, *see* DRESSLER, *supra* note 361, at 338, n.1 (citing articles).

[362] *See* Bd. of Ed. v. Earls, 122 S. Ct. 2559 (2002) (approving drug testing of all students who participate in competitive extracurricular activities); Ferguson v. Charleston, 532 U.S 67 (2001) (invalidating drug testing of maternity patients); Chandler v. Miller, 520 U.S. 305 (1997) (invalidating urinalysis requirement for candidates running for state office); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995) (upholding random drug testing of public school students who voluntarily participate athletic teams); Treasury Employees v. Von Raab, 489 U.S. 656 (1989) (upholding drug testing customs officers applying for positions involving drug interdiction or requiring the carrying of a firearm or the handling of classified documents); Skinner v. Ry. Labor Executives' Assn., 489 U.S. 602 (1989) (upholding drug and alcohol testing of railroad employees following major train accidents).

[363] *See Ferguson*, 532 U.S. at 81 (ruling unconstitutional drug testing program of maternity patients suspected of drug use primarily because the main objective of the testing was to gather evidence for law enforcement purposes); *Chandler*, 520 U.S. at 318 (invalidating statute requiring drug testing of candidates running for state office because the state had not demonstrated a substantial problem of drug abuse to justify a special need for suspicionless searches).

[364] *Earls*, 122 S. Ct. at 2565-67; *Acton*, 515 U.S. at 654-664.

compelling,"[365] especially if the facts involve a terrorist or national security threat.[366]

Based on volume alone, the drug testing cases provide considerable insight on the Justices' views about the interaction between technology and the Fourth Amendment. Therefore, lawyers and scholars may be better able to predict

[365] *Acton*, 515 U.S. at 661. The drug testing cases illustrate how the Court often finds that a challenged intrusion constitutes a search, but is nevertheless constitutionally permissible because the privacy interests and character of the intrusion are minimal. *See, e.g., Earls*, 122 S. Ct. at 2567 (explaining that "[g]iven the minimally intrusive nature of the sample collection and the limited uses to which the test results are put, we conclude that the invasion of students' privacy is not significant"); *Acton*, 515 U.S. at 658 (noting that "the privacy interests compromised by the process of obtaining the urine sample are in our view negligible"); *Skinner*, 489 U.S. at 604 (concluding that drug and alcohol testing procedures "pose only limited threats to the justifiable expectations of privacy of covered employees").

[366] *See, e.g.*, *In re*: Sealed Case No. 02-001, at 53-55, United States Foreign Intelligence Surveillance Court of Review (Decided Nov. 18, 2002), *available at* http://www.cadc.uscourts.gov/common/newsroom/02-001.pdf (relying on the Court's "special needs" cases as support for different Fourth Amendment requirements when the government's interest is to protect the nation against terrorist threats as to opposed to ordinary crime control). In theory, the "special needs" doctrine does not apply when the search promotes law enforcement interests. For example, in *Ferguson*, the Court distinguished a city hospital's drug testing of maternity patients from previously approved drug testing programs. "In each of those earlier cases, the `special need' that was advanced as a justification for the absence of a warrant or individualized suspicion was one divorced from the State's general interest in law enforcement." *Ferguson*, 532 U.S. at 79. Although "the ultimate goal of the program [in *Ferguson*] may well have been to get the women in question into substance abuse treatment and off of drugs, the immediate objective of the searches was to generate evidence *for law enforcement purposes* in order to reach that goal." *Id*. at 83-84 (footnotes omitted).

While the Court asserts that its "special needs" doctrine is inapplicable to searches that promote law enforcement objectives, its precedents suggest that this is not always the case. *See* New York v. Burger, 482 U.S. 691, 712-13 (1987) (applying "special needs" analysis and upholding statute authorizing administrative officers and *police officers* to conduct suspicionless searches of owners of automobile junkyards); *Burger*, 482 U.S. at 716 (rejecting claim that an "administrative scheme is unconstitutional simply because, in the course of enforcing it, an inspecting officer may discover evidence of crimes, besides violations of the scheme itself"); Griffin v. Wisconsin, 483 U.S. 868 (1987) (applying "special needs" analysis and upholding warrantless search of a probationer's home by a probation officer); *cf. Ferguson*, 532 U.S. at 100 (Scalia, J., dissenting) ("[S]pecial-needs doctrine was developed, and is ordinarily employed, precisely to enable searches *by law enforcement officials* who, of course, ordinarily have a law enforcement objective"); RONALD JAY ALLEN ET AL., COMPREHENSIVE CRIMINAL PROCEDURE 614 (2001) (explaining that *New York v. Burger* "most clearly illustrates the degree to which the Court is willing to recognize `special needs' in contexts where law enforcement interests are clearly also present"); DRESSLER, *supra* note 360 (acknowledging the "considerable tension between *Ferguson* and *Griffin*" on whether the presence of law enforcement interests eliminates the applicability of the "special needs" doctrine).

the Court's thinking on the "proper analytical structure that should be employed to reconcile technological change with Fourth Amendment rights"[367] by focusing on the Court's "special need" cases, rather than focusing on *Kyllo*.

CONCLUSION

The attacks of September 11 had an enormous impact on Americans' attitudes about law enforcement. After those attacks, President Bush and Congress enacted sweeping legislation designed to protect the nation from future terrorism. Much of that legislation expands the search and seizure powers of government. No one should be lulled into thinking that these expanded powers will be confined to highly-trained FBI agents investigating international terrorists. Once the judiciary approves additional search and seizure powers for federal agents, state and local police usually acquire similar authority in their fight against ordinary crime.[368] Thus, the reaction of the federal judiciary to the government's war on terrorism is likely to affect the freedom of all Americans.

It may seem unimportant to the non-lawyer whether the courts consider a particular police practice a "search" or not. But this perception is dangerous to freedom. Yale Kamisar rightly observes:

> Freedom of speech, freedom of religion, and other freedoms, have earned much praise, and deservedly so, but the Fourth Amendment may plausibly be viewed as *the* centerpiece of a free democratic society. All the other freedoms presuppose that lawless police action have been restrained. What good is freedom of speech or freedom of religion or any other freedom if law enforcement officers have unfettered power to violate a person's privacy and liberty when he sits in his home or drives his car or walks the streets?[369]

Kyllo is a significant ruling on the scope of the Fourth Amendment. Although *Kyllo*'s impact on future cases remains uncertain at this point, the choices available to the Court are

---

[367] Brochure Announcing Symposium on April 12, 2002, *The Effect of Technology on Fourth Amendment Analysis and Individual Rights*, National Center for Justice and the Rule of Law, The University of Mississippi School of Law.

[368] *See* William J. Stunz, *Local Policing After the Terror*, 111 YALE L. J. 2137, 2140 (2002) (noting that "most constitutional limits on policing are transsubstantive—they apply equally to suspected drug dealers and suspected terrorists") (footnote omitted).

[369] Yale Kamisar, *The Fourth Amendment And Its Exclusionary Rule*, THE CHAMPION Aug, 1991, at 2.

not difficult to imagine. The Court could interpret *Kyllo*'s holding as limited to a privilege against thermal imaging directed at a home. On the other hand, the Court may recognize that *Kyllo*'s logic extends to other contexts like e-mail addressing information. If the Court chooses the former interpretation, the constitutional freedoms of all Americans will be diminished.