Case Western Reserve Law Review

Volume 63 | Issue 1 Article 13

2012

I'm Not Dead Yet: *Katz*, *Jones*, and the Fourth Amendment in the 21st Century

Daniel T. Pesciotta

— Note —

I'm Not Dead Yet: *Katz*, *Jones*, and the Fourth Amendment in the 21st Century

Contents

INTRODUCTION

One would be hard pressed to find a more eloquent summation of the rights the Fourth Amendment protects than this one by Justice Brandeis:

> It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited . . . .[1]

The Fourth Amendment's goal of protecting citizen privacy "against unreasonable searches and seizures"[2] has been the major driving force behind much of the Supreme Court's Fourth Amendment jurisprudence.[3] As such, ever since the Court's seminal ruling in *Katz v. United States*, the Court has held that warrantless searches that encroach upon a citizen's reasonable expectation of privacy are unconstitutional.[4] Holding otherwise would "erode the privacy guaranteed by the Fourth Amendment."[5]

---

1. Olmstead v. United States, 277 U.S. 438, 474–75 (1928) (Brandeis, J., dissenting); *see also* 5 WILLIAM BLACKSTONE, COMMENTARIES *223 ("[T]he law of England has so particular and tender a regard to the immunity of a man's house, that it stiles it his castle, and will never suffer it to be violated with impunity.").

2. U.S. CONST. amend. IV.

3. *See, e.g.*, Katz v. United States, 389 U.S. 347, 351 (1967) ("[W]hat [citizens] seek[ ] to preserve as private, even in an area accessible to the public, may be constitutionally protected." (citations omitted)); Kyllo v. United States, 533 U.S. 27, 37 (2001) ("In the home . . . *all* details are intimate details, because the entire area is held safe from prying government eyes."); Wilson v. Layne, 526 U.S. 603, 610–11 (1999) ("[T]he 'overriding respect for the sanctity of the home that has been embedded in our traditions since the origins of the Republic' [means] that absent a warrant or exigent circumstances, police [can] not enter a home to make an arrest." (quoting Payton v. New York, 445 U.S. 573, 601 (1980))); United States v. Karo, 468 U.S. 705, 716 (1984) ("Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."); Wolf v. Colorado, 338 U.S. 25, 27 (1949) ("The security of one's privacy against arbitrary intrusion by the police—*which is at the core of the Fourth Amendment*—is basic to a free society." (emphasis added)).

4. *See Katz*, 389 U.S. at 361 (Brennan, J., concurring) ("[T]here is a twofold requirement [for determining whether a warrantless search is constitutional], first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"); *id.* at 353 (majority opinion) ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he

But despite the Court's long-established practice of protecting citizens' reasonable expectations of privacy, many commentators have expressed concern as to whether the reasonable expectation of privacy test developed in *Katz* will continue to adequately protect citizens' Fourth Amendment rights in this age of ever-advancing technology. One commentator argues that the reasonable expectation of privacy test "has proven more a revolution on paper than in practice [and] . . . [a]s a result, courts . . . have rejected broad claims to privacy in developing technologies with surprising consistency."[6] Another argues that "*Katz* was a ruling without substance" and that it has done "little to protect Fourth Amendment liberties."[7] Still other commentators argue that, in light of the privacy concerns raised by modern technology, the reasonable expectation of privacy test should be abandoned altogether.[8] Based on the tone of such commentary and the undeniably rapid advance of modern technologies, one might conclude that the death knell has already sounded for the reasonable expectation of privacy test. But contrary to such analysis, the state of the Court's Fourth Amendment jurisprudence is not as dire as some commentators make it out to be.

This Note seeks to defend the reasonable expectation of privacy test and demonstrate that it more than adequately protects citizens'

---

justifiably relied . . . and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."). The Court first used the phrase "reasonable expectation of privacy" in *Terry v. Ohio*, noting that the Court "recently held [in *Katz v. United States*] that 'the Fourth Amendment protects people, not places,' and wherever an individual may harbor a *reasonable* '*expectation of privacy*,' he is entitled to be free from unreasonable governmental intrusion." Terry v. Ohio, 392 U.S. 1, 9 (1968) (emphasis added) (citations omitted).

5. *Kyllo*, 533 U.S. at 28.

6. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 807 (2004); *see also* Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technology*, 80 MISS. L.J. 1131, 1137–38 (2011) (arguing that, while the reasonable expectation of privacy test initially seemed to promise greater Fourth Amendment protection from advancing technology, it "has not lived up to that promise for a variety of reasons, including the fact that the *Katz* test has been narrowly construed and has not easily adapted to new technologies").

7. Tracey Maclin, Katz, Kyllo, *and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 56, 58 (2002); *see also* Lewis R. Katz & Carl J. Mazzone, Safford United School District No. 1 v. Redding *and the Future of School Strip Searches*, 60 CASE W. RES. L. REV. 363, 373 (2010) ("[In the decades following *Katz*,] the Court's focus on the warrant requirement and the requirement that exigency support warrantless searches [has] faded . . . .").

8. Timothy Casey, *Electronic Surveillance and the Right to be Secure*, 41 U.C. DAVIS L. REV. 977, 1026 (2008).

Fourth Amendment rights, even in the face of rapidly advancing modern technology. Despite heavy academic criticism of the reasonable expectation of privacy test, both Supreme Court and lower federal court cases provide little reason to worry that the test is ill suited for protecting citizens' Fourth Amendment rights. Indeed, just this past term the Court held that an unwarranted search using GPS tracking technology violated the Fourth Amendment.[9] Though Justice Scalia's majority opinion reached this conclusion by relying on fundamental concepts of trespass,[10] the concurrences of Justices Sotomayor[11] and Alito[12] strongly suggest that five justices are prepared to recognize that extensive, unwarranted GPS surveillance of a citizen violates reasonable expectations of privacy.[13] Most importantly, *all nine* justices ruled in favor of protecting the defendant's Fourth Amendment rights from an advanced technology. This holding, combined with the language of many of the Court's earlier Fourth Amendment decisions, demonstrates that the reasonable expectation of privacy test is more than capable of protecting citizens' Fourth Amendment rights from such technologies.

Since the development of the reasonable expectation of privacy test in 1967, the Court has taken surprisingly few opportunities to rule on Fourth Amendment cases dealing with advanced technology. Before *Jones* in 2012 and *Kyllo v. United States*[14] in 2001, which dealt with infrared imaging, the most advanced technology the Court had dealt with in the Fourth Amendment context was aerial photography from airplanes in 1986[15] and from helicopters in 1989.[16] This absence of Supreme Court precedent dealing with truly modern technology indicates that calls for *Katz*'s demise are, at the very least, premature. It is no secret that the Court often takes its time before ruling on

9. United States v. Jones, 132 S. Ct. 945 (2012).

10. *Id.* at 952, 953 n.8 ("By attaching the device to the Jeep, officers encroached on a protected area [and thus violated the Fourth Amendment because] . . . [t]he Fourth Amendment protects against trespassory searches.").

11. *See id.* at 954–57 (Sotomayor, J., concurring).

12. *See id.* at 957–64 (Alito, J., concurring).

13. *Id.* at 964 (Alito, J., concurring) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."); *id.* at 955 (Sotomayor, J., concurring) ("I agree with Justice Alito that, at the very least, longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." (quotation marks omitted)).

14. Kyllo v. United States, 553 U.S. 27 (2001).

15. Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

16. Florida v. Riley, 488 U.S. 445 (1989).

important issues, giving the issues time to percolate in the lower courts, and the Court seems to be adopting this approach here.[17]

Further, in the only two Fourth Amendment and technology cases the Court has heard during this century, *Kyllo* and *Jones*, the Court ruled in favor of the defendant and thus actually served to *protect* citizens' privacy—not erode it. This is more evidence of the Court's steadfast adherence to the importance of protecting the privacy of citizens and indicates that the Court will continue to apply the reasonable expectation of privacy test in a manner that protects citizens' Fourth Amendment interests from modern technology.

This Note proceeds in five parts. Part I briefly explores the state of Fourth Amendment jurisprudence prior to *Katz* and the development of the reasonable expectation of privacy test. Part II then discusses the Court's seminal decision in *Katz* and interprets the reasonable expectation of privacy test. Part III surveys the Court's post-*Katz* decisions that have dealt with the Fourth Amendment and technology. Part IV analyzes the language found in many of these cases and applies it to recent scholarly criticism of *Katz* and the reasonable expectation of privacy test. Part IV concludes that these rulings indicate that the *Katz* formulation of the Fourth Amendment has and will continue to live up to the task of protecting citizens' Fourth Amendment rights from modern technology because the Court has steadfastly protected privacy in the home and has also demonstrated willingness to protect certain privacy interests outside the home as well. Part IV also examines how several lower courts have applied the reasonable expectation of privacy test in a manner that has protected Fourth Amendment rights from advancing technology. Finally, Part V briefly explores whether the judiciary or legislative branch is best suited for determining citizens' privacy rights in the face of rapidly advancing technology. Part V concludes that there are benefits and drawbacks to each branch regulating in the technology arena and recommends that decision-making power not be delegated to just one branch alone. But, since decisions pertaining to societal expectations are based largely in social policy, Part V also encourages courts applying the reasonable expectation of privacy test in new technological contexts to consider the legislative treatment of the technology in order to reach the appropriate Fourth Amendment balance.

17. *See, e.g.*, Butler v. McKellar, 494 U.S. 407, 430 n.12 (1990) (Brennan, J., dissenting) (noting that the Court typically utilizes a "process of percolation [that] allow[s] a period of exploratory consideration and experimentation by lower courts before the Supreme Court ends the process with a nationally binding rule").

I. FOURTH AMENDMENT TECHNOLOGY CASES BEFORE *KATZ*

A. The Use of Wiretapping in Olmstead v. United States

The Court's decision in *Olmstead v. United States* provides an appropriate starting point for discussing the Court's pre-*Katz* Fourth Amendment jurisprudence.[18] In *Olmstead*, the Court addressed whether warrantless wiretapping of a phone line used by suspected bootleggers violated the Fourth Amendment rights of the bootleggers who were convicted of conspiring to import, possess, and sell liquor unlawfully.[19] The bulk of the government's evidence was obtained by wiretapping the defendants' office phone and intercepting conversations about the conspiracy:

> Small wires were inserted along the ordinary telephone wires from the residence of four of the [defendants] and those leading from the chief office. The insertions were made without trespass upon any property of the defendants.[20]

In holding that the bootleggers' Fourth Amendment rights were not violated by the wiretapping, the Court noted that "[t]he [Fourth] [A]mendment . . . shows that the search is to be of material things—the person, the house, his papers, or his effects."[21] Since no "physical invasion" or seizure of "tangible material effects" occurred, the Court held that wiretapping did not implicate the Fourth Amendment:

> The reasonable view is 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. Here those who intercepted the projected voices were not in the house of either party to the conversation.[22]

At this point in the Fourth Amendment's history, the Court's jurisprudence was focused almost solely on a property-based concept of search and seizure law:

18. Olmstead v. United States, 277 U.S. 438 (1928).

19. *Id.* at 455 (the Court addressed the issue of "whether the use of evidence of private telephone conversations between the defendants and others, intercepted by means of wire tapping [sic], amounted to a violation of the Fourth and Fifth Amendments").

20. *Id.* at 456–57.

21. *Id.* at 464.

22. *Id.* at 466.

> 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.[23]

Several Justices dissented. In what is now considered a famous dissenting opinion, Justice Brandeis criticized the Court's narrow interpretation of the Fourth Amendment's language and lack of foresight into the implications advancing technology had for citizens' rights.[24] In particular, he noted that:

> [G]eneral limitations on the powers of government, like those embodied [in the Fourth Amendment], do not forbid the United States or states from meeting modern conditions by regulations which a century ago, or even a half century ago, probably would have been rejected as arbitrary or oppressive.[25]

Justice Brandeis went on to observe that our Founding Fathers "knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things" and that "[t]o protect [the Fourth Amendment rights of citizens], every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[26] Though in the minority in *Olmstead*, the emphasis Justice Brandeis placed on protecting individuals' privacy from unwarranted government intrusion would greatly influence the Court's later Fourth Amendment decisions.[27]

Justice Butler echoed Justice Brandeis's sentiments in a separate dissenting opinion, noting that "[t]he contacts between telephone

23. *Id.* at 464 (emphasis added); s*ee also* United States v. Jones, 132 S. Ct. 945, 949 (2012) (observing that the Court's "Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century").

24. Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1024 (2010); *see also infra* note 27 and accompanying text (discussing several Supreme Court cases following *Olmstead* that cited Justice Brandeis's dissent).

25. *Olmstead*, 277 U.S. at 472 (Brandeis, J., dissenting) (citations and internal quotation marks omitted).

26. *Id.* at 478.

27. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 959 (2012) (Sotomayor, J., concurring) (citing Justice Brandeis's *Olmstead* dissent to support her criticism of a purely trespass-based Fourth Amendment jurisprudence); United States v. Knotts, 460 U.S. 276, 280 (1983) (suggesting that Justice Brandeis's *Olmstead* dissent influenced the Court's decision to overturn *Olmstead* in *Katz*); Mapp v. Ohio, 367 U.S. 643, 659 (1961) (citing Justice Brandeis's *Olmstead* dissent to support the Court's application of the Fourth Amendment exclusionary rule to the states).

companies and users contemplate the private use of the facilities employed in the service."[28] He also agreed that the Court failed to appreciate the implications advancing technology had for citizens' Fourth Amendment rights:

> The direct operation or literal meaning of the words used do not measure the purpose or scope of its provisions. . . . [T]he Fourth Amendment safeguards against all evils that are like and equivalent to those embraced within the ordinary meaning of its words.[29]

B. The Use of Bugging in Goldman v. United States

Fourteen years after its ruling in *Olmstead*, the Court considered the use of a slightly different technological technique to eavesdrop on defendants and again declined to take a more expansive view of the Fourth Amendment. In *Goldman v. United States*, federal authorities had learned that the defendant was planning to commit fraud. Officers used a "detectaphone" to listen in on the defendant's phone conversations from a room adjoining his office.[30] Evidence obtained in this manner ultimately led to the defendant's conviction. On appeal, the defendant argued that when "one talks in his own office, and intends his conversation to be confined within the four walls of the room, he does not intend his voice shall go beyond those walls and it is not to be assumed he takes the risk of someone's use of a delicate detector in the next room."[31] The Court was not convinced, noting that there was no legally relevant difference between the facts of this case and those of *Olmstead*. As in *Olmstead*, the Court stressed that law enforcement officers did not trespass[32] into the defendant's office and that "[t]he listening in the next room to the words of [the defendant] as he talked into the telephone receiver was no more the interception of a wire communication . . . than would have been the overhearing of the conversation by one sitting in the same room."[33]

---

28. *Olmstead*, 277 U.S. at 487 (Butler, J., dissenting).

29. *Id.* at 488.

30. Goldman v. United States, 316 U.S. 129, 131 (1942). A "detectaphone" is essentially a large microphone held up to a wall to hear what is being said on the other side.

31. *Id.* at 135.

32. Federal agents did, at one point, trespass into the defendant's office to install a listening device. But that device did not work and thus provided the government with no evidence. This trespass bore no influence on the Court's ultimate holding. *Id.* at 131, 134–35.

33. *Id.* at 134.

Clearly the Court was still abiding by its property-based conception of the Fourth Amendment.[34]

Following in the footsteps of Justice Brandeis's *Olmstead* dissent,[35] Justice Murphy dissented in *Goldman*, pointing to the dangerous implications the Court's ruling had for the privacy rights of citizens under the Fourth Amendment: "One of the great boons secured to the inhabitants of this country by the Bill of Rights is the right of personal privacy guaranteed by the Fourth Amendment."[36] Arguing that a more liberal interpretation of the Fourth Amendment was necessary to adequately protect citizens' rights from advancing technology, Justice Murphy turned to the Founding Fathers:

> If the method and habits of the people in 1787 with respect to the conduct of their private business had been what they are today, is it possible to think that the framers of the Bill of Rights would have been any less solicitous of the privacy of transactions conducted in the office of a lawyer, a doctor, or a man of business, than they were of a person's papers and effects?[37]

Justice Murphy concluded by pointing out the narrow-mindedness of the Court's holding and again emphasizing the need to protect individual privacy: "It is a strange doctrine that keeps inviolate the most mundane observations entrusted to the permanence of paper but allows the revelation of thoughts uttered within the sanctity of private quarters, thoughts perhaps too intimate to be set down even in a secret diary . . . ."[38] Justice Murphy thus pointed out how the Court's Fourth Amendment jurisprudence was failing to protect information that citizens intended and desired to keep private.

---

34. *See supra* note 23 and accompanying text (noting the Court's Fourth Amendment jurisprudence was tied to principles of trespass until the latter half of the twentieth century).

35. *See supra* notes 24–27 and accompanying text (discussing Justice Brandeis's dissent in *Olmstead*).

36. *Goldman*, 316 U.S. at 136 (Murphy, J., dissenting). Justice Murphy even referenced Justice Brandeis's dissent in *Olmstead*, noting that he need add little more to the opposition of the majority's viewpoint than Brandeis had already done: "On the value of the right to privacy, as dear as any to free men, little can or need be added to what was said in . . . Justice Brandeis' memorable dissent in *Olmstead v. United States*." *Id.* at 137 (citation omitted).

37. *Id.* at 138–39.

38. *Id.* at 141.

II. THE DEVELOPMENT OF THE REASONABLE EXPECTATION OF PRIVACY TEST IN *KATZ*

Despite the Court's adherence to *Olmstead* in *Goldman*, the dissatisfaction with the Court's Fourth Amendment jurisprudence first expressed by Justices Brandeis, Butler, and Murphy began to take hold of other Justices. The Court began to move in a new direction with regard to the Fourth Amendment. As one commentator noted, "[w]hile the concept of 'trespassory invasions' and 'intrusions into constitutionally protected areas' may have made sense as applied to a house, a car or a briefcase, those concepts did not produce satisfactory results [in the face of] advancing technology."[39] And technology was not the only thing changing during the mid-twentieth century. Both the "legal and social climate" of the United States changed considerably in the decades following the Court's *Goldman* and *Olmstead* rulings.[40] The Supreme Court changed right along with them.[41] Under Chief Justice Warren, the Court "[became] much more willing to broadly interpret constitutional protections in the light of changing social conditions."[42] Thus, it is not surprising that the Court began "heeding Brandeis'[s] call for an explicit and robust constitutional right to personal privacy."[43]

The Court's change of direction was first signaled in *Silverman v. United States*.[44] In *Silverman*, police implanted a microphone in the defendants' house to eavesdrop on their conversations.[45] In urging the suppression of evidence obtained by this microphone, the defendants asked the Court to reexamine its previous holdings in *Olmstead* and *Goldman*.[46] The Court declined to do so, but only because "a fair reading of the record . . . show[ed] that the eavesdropping was accomplished by means of an unauthorized physical penetration into

39. Weaver, *supra* note 6, at 1150.

40. HARRY HENDERSON, PRIVACY IN THE INFORMATION AGE 66 (1999).

41. *Id.*

42. *Id.* In the 15 years prior to its ruling in *Katz*, the Court ruled on *Brown v. Board of Education*, 347 U.S. 483 (1954) (civil rights), *Mapp v. Ohio*, 367 U.S. 643 (1961) (protection against overbroad searches), *Griswold v. Connecticut*, 381 U.S. 479 (1965) (privacy), and *Miranda v. Arizona*, 384 U.S. 436 (1966) (prohibiting compelled self-incrimination), each of which represented significant expansions of citizens' rights under the Constitution.

43. HENDERSON, *supra* note 40, at 66; *see also supra* notes 24–27 (discussing Justice Brandeis's *Olmstead* dissent).

44. Silverman v. United States, 365 U.S. 505 (1961).

45. *Id.* at 506–07.

46. *Id.* at 508.

the premises occupied by the [defendants]."[47] This allowed the Court to rule in the defendants' favor by applying its property-based view of the Fourth Amendment. Addressing whether *Olmstead* and *Goldman* were still good law was not necessary.[48] Despite this, the Court hinted at its desire to expand Fourth Amendment protections and diverge from a solely property-based Fourth Amendment jurisprudence:

> It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. We find no occasion to re-examine *Goldman* here, but we decline to go beyond it, *by even a fraction of an inch.*[49]

It is also worth noting that the Court's holding in *Silverman* implicitly recognized that oral communications warranted at least some Fourth Amendment protection. The Court had declined to extend such protection to oral communications in *Olmstead* and *Goldman*.

Six years later, the Court explicitly departed from *Olmstead* and *Goldman* in the seminal case of *Katz v. United States*,[50] and established the reasonable expectation of privacy test. In *Katz*, the FBI had attached a microphone to the inside of a telephone booth that police knew a suspected gambler (Katz) frequently used.[51] Eavesdropping on Katz's phone calls confirmed the FBI's suspicions, and Katz was arrested for illegal gambling activities. His case eventually came before the Supreme Court, which addressed whether the evidence discovered by eavesdropping on Katz's telephone conversations had been obtained in violation of the Fourth Amendment.[52]

The Court rejected the government's contention that *Olmstead* and *Goldman* supported the actions of the agents, noting that "property interests" no longer "control[led]" the government's ability to conduct searches and seizures under the Fourth Amendment.[53]

47. *Id.* at 509.

48. *See id.* at 509–10 ("Eavesdropping accomplished by means of such a physical intrusion is beyond the pale of even [*Olmstead* and *Goldman*] in which a closely divided Court has held that eavesdropping accomplished by other electronic means did not amount to an invasion of Fourth Amendment rights.").

49. *Id.* at 512 (emphasis added) (citations and internal quotation marks omitted).

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

51. *Id.* at 348.

52. *Id.*

53. *Id.* at 353. In the decades following *Katz*, many commentators (and perhaps even some Justices) believed that the Court's ruling in *Katz* had done away with property law considerations in Fourth Amendment

Citing *Silverman*,[54] the Court explained that "the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any 'technical trespass under . . . local property law.'"[55] The Court also emphasized that "the Fourth Amendment protects people, not places."[56] It concluded that "the underpinnings of *Olmstead* and *Goldman* [had] been so eroded by [its] subsequent decisions that the 'trespass' doctrine there enunciated [could] no longer be regarded as controlling."[57]

Once the Court established that it would no longer follow *Olmstead* and *Goldman*, it laid the groundwork for the reasonable expectation of privacy test. "The Government's activities in electronically listening to and recording the [defendant's] words violated the *privacy upon which he justifiably relied* while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[58]

Justice Harlan concurred in the judgment, providing further clarification of the Court's holding: "My understanding of the rule that has emerged from prior decisions is that there is a twofold

---

jurisprudence altogether. *See, e.g.*, United States v. Karo, 468 U.S. 705, 712–13 (1984) ("[A]n actual trespass is neither necessary nor sufficient to establish a constitutional violation."); Kerr, *supra* note 6, at 817 ("Existing scholarship generally teaches that the Supreme Court rejected the property-based approach of *Olmstead* in 1967 when it decided *Katz v. United States*."); JEROLD H. ISRAEL & WAYNE R. LAFAVE, CRIMINAL PROCEDURE IN A NUTSHELL 60 (5th ed., 1993) ("Th[e] property approach was rejected in *Katz v. U.S.* (1967), in favor of a privacy approach.")). But the Court indicated that this was not the case just this past term in *United States v. Jones*, 132 S. Ct. 945 (2012). The majority, per Justice Scalia, noted that "*Katz* did not erode the principle 'that, when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.'" *Id.* at 951 (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring)). Further, the majority observed that "*Katz* . . . established that 'property rights are not the sole measure of Fourth Amendment violations,' but did not 'snuf[f] out the previously recognized protection for property.'" *Jones*, 132 S. Ct. at 951 (alteration in original) (quoting Soldal v. Cook County, 506 U.S. 56, 64 (1992)). As such, a warrantless search that does not violate a citizen's reasonable expectation of privacy may still violate the Fourth Amendment if the search involved trespass upon a constitutionally protected area, i.e., a person, house, paper, or effect. U.S. CONST. amend. IV.

54. Silverman v. United States, 365 U.S. 505 (1961); s*ee also supra* notes 46–52 and accompanying text (discussing *Silverman*).

55. *Katz*, 389 U.S. at 353 (citing *Silverman*, 365 U.S. at 511).

56. *Id.* at 351.

57. *Id.* at 353.

58. *Id.* (emphasis added).

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.'"[59]

The language set forth in Justice Harlan's concurrence came to be recognized as the reasonable expectation of privacy test.[60] It employs a two-pronged analysis for determining whether a warrantless search is constitutional. First, for Fourth Amendment protection to apply, the citizen must have a subjective expectation of privacy in the place or thing being searched.[61] Thus, if the subject of the search does not actually believe the place or thing being searched is private, then his rights are not violated by a warrantless search of it. Indeed, for Fourth Amendment purposes, no search is said to have occurred at all if the subject does not have a subjective expectation of privacy.[62]

Second, the subject's actual expectation of privacy must be one that society recognizes as reasonable (i.e., an objective expectation of privacy).[63] While this is an objective inquiry, it has never become totally clear how the Court answers it. Professor LaFave has speculated that the intended meaning of this prong may have been "that police investigative activity constitutes a search whenever it uncovers incriminating actions or objects which the law's hypothetical

59. *Id.* at 361 (Harlan, J., concurring).

60. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 9 (1968) (noting that the Court "held [in *Katz v. United States*] that 'the Fourth Amendment protects people, not places,' and wherever an individual may harbor a *reasonable expectation of privacy*, he is entitled to be free from unreasonable governmental intrusion" (emphasis added) (citations and internal quotation marks omitted)); United States v. Michael, 622 F.2d 744, 750 (5th Cir. 1980) (making reference to "the *Katz* reasonable expectation of privacy test, as enunciated in Mr. Justice Harlan's concurring opinion").

61. *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.1(c) (4th ed. 2011) ("In his oft-quoted concurring opinion in *Katz*, Justice Harlan stated the rule in terms of a 'two fold requirement,' the first part of which was 'that a person have exhibited an actual (subjective) expectation of privacy.'").

62. *See, e.g.*, *id.* ("There are, to be sure, a great many instances in which it is rather easy to say that *the police made no search* because the defendant surely did not actually expect privacy. If, for example, a person were openly to engage in criminal conduct in Times Square at high noon and this conduct were observed by a passing patrolman, *it could hardly be seriously claimed that this observation constituted a Fourth Amendment search.*" (emphasis added)).

63. *See id.* § 2.1(d) ("In his effort to parse the holding in *Katz*, Justice Harlan declared that the second requirement was that 'the expectation be one that society is prepared to recognize as 'reasonable.' This was apparently an attempt to give content to the word 'justifiably' in the majority's assertion that eavesdropping on Katz was a search because it 'violated the privacy upon which he justifiably relied while using the telephone booth.'").

reasonable man would expect to be private, that is, which as a matter of statistical probability were not likely to be discovered."[64] But the Court seems to have taken a slightly different approach. Justice Harlan noted in an opinion following *Katz* that this second prong involves a balancing test between citizens' "sense of security" and our nation's interest in effective law enforcement.[65] More recently, the Court noted that "what is involved here is 'our societal understanding' regarding what deserves 'protection from government invasion.'"[66] Thus, the Court seems to look primarily at two things when determining whether society is prepared to recognize an expectation of privacy as reasonable: (1) citizens' privacy interests and their need to feel secure; and (2) the importance of maintaining efficient and effective law enforcement techniques.

If the Court determines that the subject of a search did not have an objectively reasonable expectation of privacy, then no search, and thus no violation of the Fourth Amendment, is deemed to have occurred.[67]

III. FOURTH AMENDMENT TECHNOLOGY CASES AFTER *KATZ*

Since its ruling in *Katz*, the Supreme Court has decided a substantial number of Fourth Amendment cases. But surprisingly few deal with modern technology.[68] Of those, several have come out in favor of the prosecution and against a defendant seeking Fourth Amendment protection, but such results do not demonstrate a deficiency in the reasonable expectation of privacy test. The Court decided each case in a manner consistent with its well-established aim of protecting citizens' privacy through the Fourth Amendment.

64. *Id.*

65. *Id.* (quoting United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting)).

66. *Id.* (quoting Oliver v. United States, 466 U.S. 170, 178 (1984)).

67. *See, e.g.*, *id.* ("[I]t is possible that a person could reasonably rely on privacy in a given situation and, in light of all the surrounding circumstances, be unjustified. If two narcotics peddlers were to rely on the privacy of a desolate corner of Central Park in the middle of the night to carry out an illegal transaction, this would be a reasonable expectation of privacy; there would be virtually no risk of discovery. Yet if by extraordinary good luck a patrolman were to illuminate the desolate spot with his flashlight, the criminals would be unable to suppress the officer's testimony as a violation of their rights under the fourth amendment." (quoting Note, *From Private Places to Personal Privacy: A Post-Katz Study of Fourth Amendment Protection*, 43 N.Y.U. L. REV. 968, 983 (1968))).

68. *See infra* Parts III.A–E (noting that the Court has ruled on approximately eight Fourth Amendment cases involving modern technology since its ruling in *Katz*).

Accordingly, these cases do not indicate that the reasonable expectation of privacy test developed in *Katz* is unable to protect citizens' Fourth Amendment rights from modern technology.

A. Wired Informants and Pen Registers

The Court's first Fourth Amendment technology case after *Katz* was *United States v. White*.[69] In *White*, the Court addressed the admissibility of several conversations defendant White had with an undercover government agent. The undercover agent had a concealed radio transmitter on his person and transmitted the conversations to other federal agents who recorded them.[70] The Supreme Court held that the admission of these conversations at White's trial did not violate the Fourth Amendment, noting that *Katz* in no way indicated 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."[71]

The principle that disclosure to third parties limits the reasonableness of an expectation of privacy in the disclosed information was well-established precedent by the time of the Court's decision in *White*.[72] But even without such precedent, the decision was in consonance with both *Katz* and common sense. The Court noted in *Katz* that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[73] With this language in mind, it was consistent with past jurisprudence for the Court in *White* to hold that "one contemplating illegal activities must realize and risk that his companions may be reporting to the police."[74] This rule makes sense on a very basic level: once an individual converses with another, he can no longer reasonably expect the shared information to remain private because

69. United States v. White, 401 U.S. 745 (1971) (plurality opinion).

70. *Id.* at 746–47.

71. *Id.* at 749.

72. *See* Hoffa v. United States, 385 U.S. 293, 302 (1966) (when a defendant discloses information to a third party, "no interest legitimately protected by the Fourth Amendment is involved . . . [because the] Fourth Amendment [does not] protect[] a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it"); Lopez v. United States, 373 U.S. 427 (1963); s*ee also* YALE KAMISAR, WAYNE R. LAFAVE, JEROLD ISRAEL, NANCY J. KING & ORIN S. KERR, BASIC CRIMINAL PROCEDURE 474 (13th ed. 2012) ("The *Hoffa* case was decided one year before *Katz v. United States* . . . and it therefore predates the 'reasonable expectation of privacy' test first articulated in Justice Harlan's *Katz* concurrence.").

73. Katz v. United States, 389 U.S. 347, 351 (1967).

74. *White*, 401 U.S. at 752.

he cannot prevent his listener from divulging the information.[75] This principle, known as "third-party doctrine," plays a significant role in the Court's Fourth Amendment and technology jurisprudence.[76]

The Court next addressed the Fourth Amendment in a technological context eight years later in *Smith v. Maryland*.[77] This case provides an apt example of third-party doctrine in the Fourth Amendment context. The victim had been robbed by a man who drove a 1975 Monte Carlo automobile.[78] After the robbery, the victim received threatening phone calls from an individual purporting to be the robber. During one of these calls, the man told the victim to look outside. The victim saw a 1975 Monte Carlo parked outside her home. Several days later, police saw the defendant driving a 1975 Monte Carlo in the vicinity of the victim's house. Without first obtaining a warrant, the police had the telephone company install a pen register on the phone line of the car's registered owner (the defendant) in order to record the numbers dialed from his home phone. Using the information obtained from the pen register, the police determined that the defendant had indeed been placing the harassing phone calls. He was subsequently arrested and convicted of both the robbery and harassment.[79]

The Supreme Court upheld the admissibility of the pen register evidence. First, the Court noted that the defendant likely did not have even a subjective expectation of privacy because telephone users realize that they must convey "numerical information to the phone company . . . for a variety of legitimate business purposes," including long-distance billing, billing for special call plans, and preventing "unwelcome and troublesome calls."[80] Moreover, regardless of the defendant's subjective expectations, the Court held that he did not have an expectation of privacy that "society is prepared to recognize as 'reasonable.'"[81] The Court noted that it "consistently has held that

75. *See id.* at 751 ("[I]ndividual defendants neither know nor suspect that their colleagues have gone or will go to the police . . . .").

76. *See, e.g.*, Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 39 (2011) ("[T]he Fourth Amendment Third Party Doctrine . . . holds that a person retains no expectation of privacy in information conveyed to another."); *see also* Rawlings v. Kentucky, 448 U.S. 98, 105 (1980) (defendant had no reasonable expectation of privacy in drugs he placed in friend's purse because he had conveyed the drugs to a third party).

77. Smith v. Maryland, 442 U.S. 735 (1979).

78. *Id.* at 737.

79. *Id.* at 737–38.

80. *Id.* at 742–43.

81. *Id.* at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[82]

While at first glance this may seem to restrict the reasonable expectation of privacy test, the Court was careful to qualify its holding in terms of the very "limited" information pen registers record: "Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."[83] As such, the Court was careful to consider the importance of citizens' privacy before handing down its decision. In light of this qualification, it is doubtful that the Court would have upheld the use of the pen register under the reasonable expectation of privacy test if it had revealed any substance of the phone calls. Indeed, such warrantless eavesdropping was held unconstitutional in *Katz*. This holding is also faithful to the third-party doctrine rationale found in *White*. Smith could not have reasonably expected the phone numbers he dialed to remain private because a reasonable person understands that such information is conveyed to a third party.

B. The Beeper Cases

Two of the Court's most significant post-*Katz* Fourth Amendment and technology decisions occurred just a few years after *Smith*. The first case, *United States v. Knotts*,[84] involved the use of a "beeper" to track a defendant's car.[85] When federal authorities learned of an individual purchasing large amounts of chemicals typically used to manufacture methamphetamines, they installed a beeper inside a five-gallon container of chloroform, which was subsequently sold to the defendant.[86] Through a combination of visual surveillance and tracking information transmitted by the beeper, officers tracked the defendant's car to a cabin in a remote part of Minnesota. No information from the beeper was used after the location of the cabin was determined.[87] Police subsequently discovered that the defendant

82. *Smith*, 442 U.S. at 743–44 (citing United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion), Hoffa v. United States, 385 U.S. 293, 302 (1966), and several other Supreme Court decisions).

83. *Smith*, 442 U.S. at 741–42.

84. United States v. Knotts, 460 U.S. 276 (1983).

85. The "beeper" utilized by law enforcement in this case was a sort of tracking device. *See id.* at 277 ("A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver.").

86. Police received permission from the chemical company before installing the beeper in the container of chloroform. *Id.* at 278.

87. *Id.* at 278–79.

had a drug lab and fourteen pounds of pure amphetamine in the cabin. The defendant was arrested and convicted on drug charges.[88]

The Supreme Court held that the surveillance information provided by the beeper did not violate the Fourth Amendment.[89] The Court's holding was based primarily on its conclusion that citizens do not have a reasonable expectation of privacy in their movements when driving in an automobile:

> A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.[90]

As in *Smith*, the Court was careful to qualify its holding, noting that "there [was] no indication that the beeper was used in any way to reveal information as to the movement of the [chemicals] within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin."[91] Thus, the Court applied third-party doctrine in a manner similar to that in *White* and *Smith*, but was careful to note that its holding may well have been different if the beeper had revealed information not already made available to the general public.

The following year, in *United States v. Karo*,[92] the Court demonstrated the limits of its holding in *Knotts*. The facts of *Karo* were remarkably similar to those of *Knotts*. Federal agents learned that the defendant was buying large amounts of ether, a chemical used to extract cocaine from clothing.[93] After obtaining the chemical seller's consent, agents replaced one of the barrels in the defendant's upcoming order with a barrel containing a hidden beeper.[94] Agents observed the defendant pick up the barrels and used the beeper to track them back to the defendant's house. At this point, the facts began to differ from those of *Knotts*. Over the next several months,

88. *Id.* at 279.

89. As it was not an issue raised on appeal, the Court did not address whether the initial installation of the beeper violated the defendant's Fourth Amendment rights. *Id.* at 279 n.*.

90. *Id.* at 281–82.

91. *Id.* at 285.

92. United States v. Karo, 468 U.S. 705 (1984).

93. *Id.* at 708.

94. *Id.*

agents continued to use the beeper, determining that the ether was moved to three other houses and two different storage facilities.[95] Five months after the defendant first picked up the barrel, agents tracked it, still using the signals transmitted by the beeper, to a house rented by the defendant.[96] The following day, agents used the beeper to determine that the barrel was still on the premises and also noted that the house's windows were open despite it being a very cold day.[97] Based on this information, agents acquired a search warrant and discovered a cocaine laboratory in the house. The defendant was arrested and convicted of conspiracy to possess cocaine.[98]

The Supreme Court overturned the defendant's conviction. Distinguishing *Knotts*, the Court noted that the beeper in *Karo* "was used to locate the ether in a specific house."[99] In comparison, the beeper in *Knotts* had been used only to track a car to a specific location, using information that was "'voluntarily conveyed to anyone who wanted to look.'"[100] Since the beeper in *Karo* was used to "reveal a critical fact about the interior of the premises . . . that [the Government] could not have otherwise obtained without a warrant,"[101] the Court held that the police had infringed upon the defendant's reasonable expectation of privacy within his residence:

> [P]rivate residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable . . . . Indiscriminate 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.[102]

As such, the Court demonstrated the limit of third-party doctrine. The beeper tracking in *Karo* went beyond simply helping the police discover information that was already being conveyed to the public. It helped them discover information that they could not have otherwise discovered without encroaching upon the defendant's reasonable expectation of privacy in his house. While citizens oftentimes cannot

95. *Id.* at 708–10.

96. *Id.* at 709.

97. *Id.* at 710.

98. *Id.*

99. *Id.* at 714.

100. *Id.* at 715 (citing United States v. Knotts, 460 U.S. 276, 281 (1983)).

101. *Karo*, 468 U.S. at 715.

102. *Id.* at 714, 716.

reasonably expect to keep private that which they expose to the public, the Court recognized that it is most certainly reasonable to expect privacy for that which goes on behind closed doors in a home.

C. Aerial Surveillance

In 1986, the Court ruled on two Fourth Amendment cases involving aerial surveillance. The first, *California v. Ciraolo*,[103] involved a defendant who grew large quantities of marijuana in his backyard. Since the defendant's yard was surrounded by a ten-foot-high fence, police flew a plane over his house and took pictures of his marijuana crop.[104] The police used these pictures to obtain an arrest warrant and, after failing to get the pictures suppressed, the defendant pled guilty to the cultivation of marijuana.[105]

The Supreme Court held that the aerial surveillance did not violate the defendant's rights. While acknowledging that the "curtilage" of one's property is generally protected under the Fourth Amendment,[106] the Court made clear that "[t]he Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."[107] As such, the Court held that the defendant's "expectation that his garden was protected from . . . observation was unreasonable" because "[a]ny member of the public flying in [the] airspace [above the defendant's yard] . . . could have seen everything that these officers observed."[108] Such reasoning may initially seem to stretch the bounds of third-party doctrine—indeed, what are the chances a member of the general public would fly over the defendant's house and identify as marijuana the plants growing in his backyard?[109]

103. California v. Ciraolo, 476 U.S. 207, 209 (1986).

104. *Id.*

105. *Id.* at 209–10.

106. *See, e.g.*, Oliver v. United States, 466 U.S. 170, 180 (1984) ("[C]urtilage . . . warrants the Fourth Amendment protections that attach to the home. At common law, 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 considered part of home itself for Fourth Amendment purposes." (citation and internal quotation marks omitted)).

107. *Ciraolo*, 476 U.S. at 213.

108. *Id.* at 213–14.

109. *See id.* at 224 (Powell, J., dissenting) ("The only possible basis for [the Court's holding] is a judgment that the risk to privacy posed by the remote possibility that a private airplane passenger will notice outdoor activities is equivalent to the risk of official aerial surveillance . . . . Members of the public use the airspace for travel, business, or pleasure, not for the purpose of observing activities taking place within residential yards.").

But the Court further clarified the unreasonableness of the defendant's expectation of privacy in this case, noting that even a "power company repair mechanic on a pole overlooking the yard" could have seen the marijuana.[110] Presumably, one of the defendant's neighbors could also have seen over the fence by looking out a second-story window into the backyard.

In fact, a neighbor looking into Ciraolo's yard may have been precisely what happened. The officer in charge of the search had over eight years of experience dealing with and identifying marijuana gardens and had received an anonymous phone call in which the caller stated he could see marijuana in Ciraolo's backyard.[111] That officer also received "ten to twelve" other tips about marijuana gardens in the same general area as Ciraolo's house, and during the aerial surveillance at issue in the case the officer identified five other marijuana gardens in addition to Ciraolo's.[112] The Court's opinion inexplicably omitted these facts, based on which it appears that the flight was not undertaken solely to peer into a single citizen's backyard, but rather as a part of a larger-scale investigation.

Viewed in light of these facts, the Court's holding in *Ciraolo* is not surprising. When one conducts illegal activities in his backyard with nothing more than a fence separating him from the public eye, it is unreasonable to believe that the activities will go undetected by individuals outside the property. Further, evidence of Ciraolo's criminal activity was obtained during a sweep of an entire area—an area that police arguably had at least reasonable suspicion, and perhaps even probable cause, to believe was a hotbed of drug-related activity.

On the same day it decided *Ciraolo*, the Court also handed down its decision in *Dow Chemical Co. v. United States*,[113] a case with largely parallel facts. After the Dow Chemical Company refused to admit EPA inspectors into its factory, the EPA employed a professional aerial photographer to fly over the plant and take pictures of it.[114] The EPA did not inform Dow Chemical of this surveillance, and when Dow found out it filed suit against the EPA, alleging (among other things) a violation of the Fourth Amendment. The Supreme Court held that no such violation had taken place and rejected Dow Chemical's argument that the outdoor areas surrounding its enclosed

110. *Id.* at 215 (majority opinion).

111. Brief of Petitioner-Appellant at 6–8, California v. Ciraolo, 476 U.S. 207 (1986) (No. 84-1513) (Aug. 8, 1985).

112. *Id.* at 8. The impressive size of the marijuana crop is revealed in the petitioner's brief: "Seventy three cultivated marijuana plants, averaging eight feet tall, were seized from [Ciraolo's] back yard." *Id.* at 10.

113. Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

114. *Id.* at 229.

buildings were "industrial curtilage."[115] The Court noted that these areas were more akin to "open fields" than curtilage and thus were not protected by the Fourth Amendment: "The intimate activities associated with family privacy and the home and its curtilage simply do not reach the outdoor areas or spaces between structures and buildings of a manufacturing plant . . . . [W]hat is observable by the public is observable without a warrant, by the Government inspector as well."[116]

While the Court could have ended its decision there, it went on to clarify the narrowness of its holding. It emphasized that the inner areas of Dow Chemical's plant were clearly protected by the Fourth Amendment, but noted that the owner of commercial property cannot expect the same level of privacy as a homeowner in his dwelling since commercial properties, unlike homes, are not "free from any inspections."[117] The Court also suggested that the use of highly advanced technology to conduct searches "might be constitutionally proscribed absent a warrant."[118] Its holding may have been different had the camera used in the case been able to reveal intimate details like a "class ring" or "identifiable human faces."[119] Such circumstances would have "implicate[d] more serious privacy concerns."[120]

D. Infrared Imaging

In 2001, the Court ruled on *Kyllo v. United States*.[121] Federal agents received a tip that the defendant grew marijuana in his home. Since such indoor cultivation typically entails the use of high-intensity lamps, police used a thermal imager to determine whether high levels of heat were emanating from the defendant's house.[122] The scans revealed that parts of the house were significantly warmer than the surrounding homes. This evidence helped the police obtain a search warrant and ultimately discover the defendant's marijuana plants. After unsuccessfully moving to suppress the thermal imaging evidence, the defendant conditionally pled guilty to manufacturing marijuana.[123]

115. *Id.* at 235.

116. *Id.* at 236, 238 (internal quotation marks omitted).

117. *Id.* at 238.

118. *Id.*

119. *Id.* at 238, n.5.

120. *Id.*

121. Kyllo v. United States, 533 U.S. 27 (2001).

122. *Id.* at 29–30.

123. *Id.* at 30.

The Court held that the defendant's Fourth Amendment rights had been violated by the admission of the thermal imaging evidence. It began by emphasizing that "[w]ith few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no."[124] After recognizing the dangers modern technology poses to the privacy of citizens,[125] the Court went on to hold 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."[126]

The Court made the need to ensure that citizens' rights are adequately protected from advancing technology abundantly clear in its decision. It pointed out the dangers posed to privacy rights by devices like "thermal imager[s]," "powerful directional microphone[s]," and "satellite[s]" and stated that "the rule we adopt must take account of more sophisticated systems that are already in use or in development."[127] The Court explicitly rejected the suggestion of limiting the Fourth Amendment to prohibiting only those practices that reveal "intimate details" of the household.[128] The Court observed that "[i]n the home . . . *all* details are intimate details, because the entire area is held safe from prying government eyes" and that "the Fourth Amendment draws a firm line at the entrance to the house."[129] The Court could not have made clearer its dedication to protecting the privacy of the home.

E. GPS Surveillance: United States v. Jones

This past term, the Court handed down its most recent Fourth Amendment and technology decision, *United States v. Jones*.[130] Jones was suspected of trafficking drugs. Without a warrant,[131] police attached a GPS tracking device to the underside of his car and tracked its movements for twenty-eight days, generating over 2,000 pages of data.[132] The government eventually used this information to

124. *Id.* at 31.

125. *See id.* at 33–34 ("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.").

126. *Id.* at 34 (citation and internal quotation marks omitted).

127. *Id.* at 35–36.

128. *Id.* at 37–38.

129. *Id.* at 37, 40 (citation and internal quotation marks omitted).

130. United States v. Jones, 132 S. Ct. 945 (2012).

131. The police actually did obtain a warrant at one point, but it expired prior to their installation of the GPS device on Jones's car. *Id.* at 948.

132. *Id.*

charge Jones with multiple counts of conspiracy to possess and distribute cocaine.[133] Jones unsuccessfully moved the district court to suppress the GPS evidence and was ultimately convicted on the drug charges.[134] The United States Court of Appeals for the District of Columbia Circuit reversed Jones's conviction and suppressed the GPS evidence, noting that "[a] reasonable person does not expect anyone to monitor and retain a record of every time he drives his car . . . [because] prolonged GPS monitoring defeats an expectation of privacy that our society recognizes as reasonable."[135]

The Supreme Court, per Justice Scalia, affirmed the Court of Appeals' result, but on different grounds. Since the government "physically occupied" a Fourth Amendment "effect" without first obtaining a warrant, the Court held that it did not even need to pursue a *Katz* reasonable expectation of privacy analysis to conclude that Jones's Fourth Amendment rights had been violated.[136] Protecting "effects" from unwarranted government intrusions was a function of the Fourth Amendment even before the adoption of the reasonable expectation of privacy test. The Court admonished that "*Katz* did not repudiate [this] understanding" and "did not erode the principle 'that, when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.'"[137]

The Court made clear that its ruling in *Katz* was an expansion of Fourth Amendment protections[138] and "*added to*, not *substituted for*, the common-law trespassory test."[139] Thus, the Court held that when the government intrudes upon an area explicitly protected by the Fourth Amendment for the purpose of obtaining information, that action is a prima facie unconstitutional search if done without a warrant. *Katz* analysis is not even necessary to protect such a basic Fourth Amendment guarantee.

133. *Id.* at 948–49.

134. *Id.* at 949.

135. United States v. Maynard, 615 F.3d 544, 563, 565 (D.C. Cir. 2010), *aff'd on other grounds sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

136. *Jones*, 132 S. Ct. at 950–52.

137. *Id.* at 950–51 (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring)).

138. *Jones*, 132 S. Ct. at 951 ("*Katz* did not narrow the Fourth Amendment's scope."); *see also id.* at 955 (Sotomayor, J., concurring) ("In *Katz*, [the] Court *enlarged* its then-prevailing focus on property rights by announcing that the reach of the Fourth Amendment does not 'turn upon the presence or absence of a physical intrusion.'" (emphasis added)).

139. *Id.* at 952 (majority opinion).

Though not necessary to its holding, the Court also included some discussion about the reasonable expectation of privacy test and the need to protect citizens' privacy interests. The Court noted that "[s]ituations involving merely the transmission of electronic signals without trespass *remain* subject to *Katz* analysis."[140] The majority reaffirmed the Court's dedication to protecting privacy interests, stating that "[a]t bottom, [the Court] must 'assur[e] preservation of that degree of *privacy* against government that existed when the Fourth Amendment was adopted.'"[141] A search similar to the one in *Jones*, but achieved "without an accompanying trespass, [may be] an unconstitutional invasion of privacy."[142] "*Katz* analysis" would be used to answer such a question should it arise.[143] This language makes clear that the Court intends to continue utilizing the reasonable expectation of privacy test in future Fourth Amendment and technology cases.

An intriguing duo of concurrences further demonstrates the reasonable expectation of privacy test's continued vitality in the technology context. Justice Sotomayor joined the majority's opinion because the government's intrusion upon a constitutionally protected area allowed for resolution of this case on a "narrow[ ] basis."[144] She recognized the trespassory test espoused by the majority as an "irreducible constitutional minimum."[145] But she also wrote separately to acknowledge the potential threats posed to the Fourth Amendment by GPS technology. She noted that, since "physical intrusion is now unnecessary to many forms of surveillance," the Court will have to rely largely on *Katz* analysis in future Fourth Amendment cases.[146] Justice Sotomayor went on to argue that it would be important to account for the "substantial quantum of intimate information" revealed by advanced surveillance technologies like GPS when applying the *Katz* test in future cases: "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[147] To support this argument, she pointed out that the

140. *Id.* at 953.

141. *Id.* at 950 (emphasis added) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

142. *Jones*, 132 S. Ct. at 954.

143. *Id.*

144. *Id.* at 957 (Sotomayor, J., concurring).

145. *Id.* at 955.

146. *Id.*

147. *Id.* at 956.

Court left open in *Kyllo* the possibility that "duplicating traditional surveillance 'through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy.'"[148] Thus, it appears Justice Sotomayor is prepared to hold in future cases that unwarranted GPS surveillance infringes upon citizens' reasonable expectations of privacy.

Justice Alito wrote a separate concurring opinion, joined by Justices Ginsburg, Breyer, and Kagan. He seemed largely to agree with Justice Sotomayor's view, arguing that long-term "GPS monitoring in investigations of most offenses impinges on expectations of privacy."[149] He noted that "[f]or such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[150] Therefore, at least as far as *long-term* GPS surveillance is concerned, Justice Alito, along with Justices Ginsburg, Breyer, and Kagan, would hold that such an investigative technique fails *Katz* analysis and thus violates the Fourth Amendment.[151]

The disjoint between Justices Alito and Sotomayor resulted from Justice Alito's argument that "relatively short-term [GPS] monitoring of a person's movements on public streets" does not violate a reasonable expectation of privacy.[152] He also does not buy into the trespassory test espoused by the majority.[153] In contrast, Justice Sotomayor agrees with the majority holding, noting that "Justice Alito's approach, which discounts altogether the constitutional relevance of the Government's physical intrusion on Jones' Jeep, erodes that longstanding protection for privacy inherent in items of property that people possess or control."[154] She also seems to believe that, due to the invasive nature of GPS surveillance, all such surveillance implicates a reasonable expectation of privacy.[155]

148. *Id.* (quoting Kyllo v. United States, 533 U.S. 27, 35 n.2 (2001)).

149. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

150. *Id.*

151. Justice Alito did not make clear what his definition of "long-term" is. *See id.* ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4 week mark."); *see also id.* at 954 (majority opinion) ("[I]t remains unexplained why a 4 week investigation is 'surely' too long.").

152. *Id.* at 964 (Alito, J., concurring); *see also infra* notes 276–82 and accompanying text (discussing the concurring opinions in *Jones*).

153. *See Jones*, 132 S. Ct. at 957–64 (Alito, J., concurring).

154. *Id.* at 955 (Sotomayor, J., concurring).

155. *Id.*

There are two key points to take away from *Jones*. First, in a case involving by far the most advanced surveillance technology the Court has dealt with, *all nine* justices voted to protect citizens' Fourth Amendment rights. Second, and perhaps more importantly for the purposes of this Note, five justices also indicated that, at least as far as long-term GPS surveillance is concerned, they are prepared to apply the reasonable expectation of privacy test in a manner that recognizes society's reasonable expectation that it will not be continuously monitored by GPS technology. This apparent willingness strongly indicates that the reasonable expectation of privacy test can be applied in a way that protects citizens' Fourth Amendment rights from the advance of modern technology.

IV. *KATZ* LIVES

Academic reception of *Katz's* reasonable expectation of privacy test has been lackluster at best. One commentator, although characterizing the holding of *Katz* as "revolutionary," argues that "the passage of time . . . [has] show[n] that *Katz* . . . [has done] little to protect Fourth Amendment liberties."[156] Other commentators have criticized *Katz* for being ambiguous and failing to provide adequate guidance as to how the reasonable expectation of privacy test ought to be applied.[157] With regard to the Fourth Amendment and modern technologies, commentators have argued that the reasonable expectation of privacy test in its current state is insufficient to protect citizens from warrantless e-mail searches[158] and video surveillance.[159]

156. Maclin, *supra* note 7, at 56; *see also* Donald L. Doernberg, *"Can You Hear Me Now?": Expectations of Privacy, False Friends, and the Perils of Speaking Under the Supreme Court's Fourth Amendment Jurisprudence*, 39 IND. L. REV. 253, 255 (2006) ("The Court needs to reconsider how expectations of privacy really work."); Kerr, *supra* note 6, at 807 (arguing that the reasonable expectation of privacy test "has proven more a revolution on paper than in practice").

157. *See, e.g.*, Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1366 (2004) ("[*Katz's*] ambiguity blurs the clear lines people often depend on to figure out where and when they are free from monitoring and leads courts to confuse situations where privacy interests are absent with very different situations where privacy interests must share space with other important public interests, but deserve vigorous protection at the same time."); James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 340 (2002) ("bemoan[ing] the serious deficiencies in the guidance provided by the *Katz* opinion" and arguing that "[t]he Court provided little, if any, insight concerning [the] critical issue[ ]" of what privacy interests are actually protected by the Constitution).

158. *See* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56

Several commentators have even proposed doing away with the reasonable expectation of privacy test all together.[160] Some of the initial reaction to *United States v. Jones* seems to suggest that many of these commentators won't be changing their minds anytime soon.[161]

Despite such negative commentary, significant evidence indicates that the reasonable expectation of privacy test has more than

---

MERCER L. REV. 507, 522 (2005) ("[M]ost courts have yet to determine whether the sender of e-mail retains a reasonable expectation of privacy in the contents of the message. An examination of how the [reasonable expectation of privacy] doctrine applies to e-mail demonstrates an ambiguity in the third party doctrine that has significant ramifications for technologically-enhanced searches."); Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 814 (2003) ("[T]he answer to the question of how much privacy protection the Fourth Amendment guarantees to Internet communications appears to be 'not much.' And certainly not enough."); Ryan A. Ray, *The Warrantless Interception of E-Mail: Fourth Amendment Search or Free Rein for the Police?*, 36 RUTGERS COMPUTER & TECH. L.J. 178, 181 (2010) ("It seems that most, if not all, e-mail users expect that their e-mail will remain private, at least until the messages reach the intended recipient . . . . Yet many courts have refused to recognize e-mail users' expectations of privacy.").

159. Blitz, *supra* note 157. *See also* Casey, *supra* note 8, at 977 ("The application of the *Katz* standard . . . has generated anomalous results, and the deficiencies of the *Katz* test are particularly apparent in the context of the government's use of new technologies to conduct electronic surveillance.").

160. *See* Casey, *supra* note 8, at 1026 ("The reasonable expectation of privacy standard should be abandoned in favor of a test that reclaims the original language of the Fourth Amendment—the right to be secure. Removing the reasonable expectation of privacy from our Fourth Amendment discourse will resolve some of the confusion that has plagued jurisprudence in the post-*Katz* era."); Henderson, *supra* note 158, at 546 (arguing in favor of "jettisoning the [reasonable expectation of privacy] test in favor of a dictionary definition of search"); Kerr, *supra* note 6, at 807 (arguing that courts "have rejected broad claims to privacy in developing technologies with surprising consistency" and urging that courts should take a backseat to the legislature in making Fourth Amendment decisions dealing with technology); Steven Penney, *Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach*, 97 J. CRIM. L. & CRIMINOLOGY 477, 506 (2007) (arguing that the reasonable expectation of privacy test should be replaced with an "economically-informed cost-benefit analysis"); s*ee also* Kerr, *supra* note 24 (proposing a new test for dealing with searches of e-mail).

161. *See, e.g.*, Barry Friedman, Op-Ed., *Privacy, Technology, and Law*, N.Y. TIMES, Jan. 29, 2012, at SR5 ("*Jones*, along with other recent decisions, may turn the Fourth Amendment into a ticking time bomb, set to self-destruct—and soon—in the face of rapidly emerging technology."); s*ee also infra* Part IV.B.4 (discussing the impact of *Jones* on Fourth Amendment jurisprudence).

adequately protected citizens' privacy interests in the past and that it will continue to do so—even in the face of advancing technology. The Supreme Court's own Fourth Amendment jurisprudence supports this proposition.[162] Further, lower courts have dealt with several types of modern technology that the Supreme Court has yet to pass judgment on and have utilized the reasonable expectation of privacy test to protect the privacy interests of citizens.[163] As such, recommendations that the Court abandon *Katz* and the reasonable expectation of privacy test in the face of advancing technology would seem at the very least premature, and, as shown below, completely unnecessary.

A. A Lack of "Modern" Technology Fourth Amendment Cases

Before analyzing the Supreme Court's Fourth Amendment jurisprudence, it is important to point out that the Court has ruled on an extremely small number of Fourth Amendment cases dealing with modern technology. Before the Court's ruling in *Jones*[164] this past term, *Kyllo* was the Court's only Fourth Amendment case substantively involving some sort of modern technology in the past twenty years.[165] Many rapidly advancing technologies with serious Fourth Amendment implications, such as video surveillance,[166] have yet to come before the Court in any Fourth Amendment context. Perhaps most notably, and despite extensive academic condemnation of the reasonable expectation of privacy test in the realm of the Internet,[167] the Court has *never* ruled on a Fourth Amendment case dealing with a search of information on the Internet.

---

162. *See infra* Part IV.B (demonstrating how the Court's Fourth Amendment jurisprudence indicates that the reasonable expectation of privacy is capable of protecting citizens' privacy interests).

163. *See infra* Part IV.C (discussing lower courts' application of the reasonable expectation of privacy test).

164. United States v. Jones, 132 S. Ct. 945 (2012); *see also supra* Part III.E (discussing the holding of, and concurring opinions in, *Jones*).

165. Kyllo v. United States, 533 U.S. 27 (2001) (holding that the warrantless use of infrared technology to detect heat emanating from defendant's townhouse violated the defendant's reasonable expectation of privacy and thus was an impermissible search under the Fourth Amendment); *see supra* Part III.D (discussing the holding of *Kyllo*). In 2010, the Court dealt with a case involving text messaging and the Fourth Amendment. But the Court sidestepped the technological issue entirely by deciding the case under already established principles of Fourth Amendment and employment law. *See* City of Ontario v. Quon, 130 S. Ct. 2619 (2010). That the Court opted to do so is yet another instance of the Justices approaching modern technology in the Fourth Amendment context with caution.

166. *See infra* Part IV.C.1.

167. Kerr, *supra* note 6; Kerr, *supra* note 24; Maclin, *supra* note 7; s*ee also* Peter P. Swire, *Katz is Dead. Long Live Katz*, 102 MICH. L. REV. 904,

From these considerations alone, this Note urges patience on the part of Fourth Amendment commentators. It is no secret that the Court prefers to let issues percolate in the district and circuit courts before definitively ruling on them[168] and often feels bound by judicial restraint to rule only on matters immediately before it.[169] The Court has been particularly inclined toward this practice in the law and technology context.[170] For this reason, it is as of yet unclear how the Court will apply the reasonable expectation of privacy test to many of the new technologies of the past twenty years, meaning that the call for *Katz's* demise has been, at the very least, premature. In the meantime, commentators concerned about poorly reasoned lower court opinions unduly influencing the Supreme Court should take solace in the fact that in *Kyllo* the Court granted a criminal suspect "a protection previously rejected by five federal courts of appeals and

904 (2004) ("[T]he demise of *Katz* has actually been understated. . . . [C]ases . . . hold that many kinds of surveillance are not 'searches' under the Fourth Amendment."); Matthew D. Lawless, Comment, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 11 UCLA J.L. & TECH., no. 1, Spring 2007, at 1, *available at* http://www.lawtechjournal.com/articles/2007/02_070426_lawless.pdf ("[T]he only bar to [Internet search] records becoming Exhibits A-Z [in a criminal proceeding] is a Fourth Amendment that, while purporting to protect expectations of privacy society would deem reasonable, utterly fails to consider what society has said about Internet searches.").

168. *See, e.g.*, Butler v. McKellar, 494 U.S. 407, 430–31 n.12 (1990) (Brennan, J., dissenting) (noting that the Court typically utilizes a "process of percolation [that] allow[s] a period of exploratory consideration and experimentation by lower courts before the Supreme Court ends the process with a nationally binding rule" (quoting Samuel Estreicher & John E. Sexton, *A Managerial Theory of the Supreme Court's Responsibilities: An Empirical Study*, 59 N.Y.U. L. REV. 681, 716 (1984))).

169. *See, e.g.*, Ashwander v. Tenn. Valley Auth., 297 U.S. 288, 341 (1936) (Brandeis, J., concurring) ("Considerations of propriety, as well as long-established practice, demand that [the Court] refrain from passing upon the constitutionality of an [issue] unless obliged to do so in the proper performance of our judicial function, when the question is raised by a party whose interests entitle him to raise it." (quoting Blair v. United States, 250 U.S. 273, 279 (1919))).

170. *See, e.g.*, *Quon*, 130 S. Ct. at 2629 ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. . . . Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.").

adopted by none."[171] Further, substantial evidence in the jurisprudence of both the Supreme Court and the lower courts suggests the reasonable expectation of privacy test provides a more than satisfactory framework for protecting citizens' Fourth Amendment privacy rights in the face of advancing technology.

B. Katz *and the Protection of Citizens' Privacy*

1. Unwavering Protection of the Home

Ample language exists in the Supreme Court's Fourth Amendment decisions to suggest that, as the Court begins to hear more Fourth Amendment cases dealing with modern technology, it will apply the reasonable expectation of privacy test in a manner that protects citizens' privacy. First and foremost, the Court has always been steadfast in its protection of privacy in the home—an area in which all citizens undoubtedly expect the utmost level of privacy. As early as 1886, the Court recognized that the Fourth Amendment "appl[ies] to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life."[172] The Court has never wavered from this principle. In *Karo*, the Court recognized as a "basic Fourth Amendment principle" that "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant."[173] In language undoubtedly referencing *Katz's* reasonable expectation of privacy test, the Court noted that this "expectation is plainly one that society is prepared to recognize as justifiable."[174] With this language in hand, the Court went on to hold in *Karo* that beeper tracking technology could not be used without a warrant to "reveal a critical fact about the interior of [a house] that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant."[175]

More recently, the Court dealt with infrared technology in *Kyllo*.[176] Staying true to its emphasis on protecting the privacy of the home, the Court, per Justice Scalia,[177] noted that "'[a]t the very core'

171. David A. Sklansky, *Back to the Future:* Kyllo*,* Katz*, and Common Law*, 72 MISS. L.J. 143, 144 n.5 (2002) (citing multiple circuit court cases holding that the use of warrantless thermal imaging did not violate the Fourth Amendment).

172. Boyd v. United States, 116 U.S. 616, 630 (1886).

173. United States v. Karo, 468 U.S. 705, 714 (1984).

174. *Id.*

175. *Id.* at 715.

176. Kyllo v. United States, 533 U.S. 27 (2001).

177. The fact that Justice Scalia penned the majority opinion in *Kyllo* should not be overlooked. Prior to the *Kyllo* decision, Justice Scalia had been

of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'"[178] The Court went on to cite the reasonable expectation of privacy test, stating that

> the Fourth Amendment draws a firm line at the entrance of the house . . . . In the case of the search of the interior of homes . . . there is a ready criterion, with roots deep in the common law, of the minimal *expectation of privacy* that *exists*, and that is acknowledged to be *reasonable*.[179]

The Court ultimately held that the warrantless use of infrared technology to detect temperature levels in the defendant's house was contrary to the Fourth Amendment. All details of the home's interior, the Court noted, are protected "from prying government eyes" under the Fourth Amendment.[180] The Court used *Kyllo* to draw "a firm line at the entrance of the house" to ensure that law enforcement cannot use advanced technology to intrude upon the most private of all places—the home.[181]

The language and holdings of cases like *Karo* and *Kyllo* make abundantly clear that the Court has successfully used the reasonable expectation of privacy test to defend citizens' privacy interests in their homes from invasive modern technologies. This is of the utmost importance. Throughout this nation's history, and indeed even well

---

one of the reasonable expectation of privacy test's most outspoken critics. For instance, just a few years prior he had characterized the reasonable expectation of privacy test as "self-indulgent" and lacking "plausible foundation in the text of the Fourth Amendment." Minnesota v. Carter, 525 U.S. 83, 97 (1998). While the test did not completely escape criticism in his majority opinion (he noted that the test has "often been criticized as circular," *Kyllo*, 533 U.S. at 34), Justice Scalia clearly applied the reasonable expectation of privacy test in holding that the government's warrantless use of thermal imaging violated the defendant's reasonable expectation of privacy as to the intimate details of his home. *See also* Tomkovicz, *supra* note 157, at 343 n.126 (discussing Justice Scalia's concurrence in *Minnesota v. Carter*).

178. *Kyllo*, 533 U.S. at 31 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

179. *Kyllo*, 533 U.S. at 34, 40 (emphasis added) (citation and internal quotation marks omitted).

180. *Id.* at 37. Justice Breyer was particularly concerned about protecting the interior of the home from prying eyes. At the oral argument for *Kyllo*, he quipped: "I usually spend three or four hours a day in my Finnish sauna. People think I'm working. I don't want them to find out what's going on." Transcript of Oral Argument at 37, Kyllo v. United States, 533 U.S. 27 (2001) (No. 99–8508), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/99-8508.pdf.

181. *Kyllo*, 533 U.S. at 40.

before it,[182] the home has been considered a "sacred" place, "a haven from the anxieties of modern life . . . [that provides] a shelter for . . . moral and spiritual values."[183] The importance of having a home that one can retreat to for privacy has been recognized by virtually all facets of American culture; everything from books[184] and movies[185] to zoning[186] and tort law[187] place high value on the home as

182. *See, e.g.*, John M. Roberts & Thomas Gregor, *Privacy: A Cultural View*, *in* PRIVACY 199–200, 203 (J. Roland Pennock & John W. Chapman eds., 1971) ("[T]he household is truly a cultural universal. . . . Societies differ in many ways, but they always have households of one sort or another. . . . It would appear that privacy, as we know it, is largely a neolithic invention occurring primarily in the Old World and associated with the Near Eastern cultural complex which later diffused to all the centers of high culture in the Old World."). The late law professor and former chief counsel for the U.S. Senate Watergate Committee, Samuel Dash, explored the legal history of privacy in his book *The Intruders.* SAMUEL DASH, THE INTRUDERS: UNREASONABLE SEARCHES AND SEIZURES FROM KING JOHN TO JOHN ASHCROFT (2004). In the book's introduction, Professor Dash pointed to several famous men throughout history whose words demonstrate the long-cherished history of the home as a haven, including William Pitt, Hammurabi, and Cicero. *Id.* at 1, 9. William Pitt offered the famous refrain:

> The poorest man may, in his cottage, bid defiance to all the forces of the Crown. It may be frail—its roof may shake—the wind may blow through it—the storm may enter—the rain may enter—but the King of England may not enter!—all his force dare not cross the threshold of the ruined tenement!

HISTORICAL SKETCHES OF STATESMAN WHO FLOURISHED IN THE TIME OF GEORGE III 42 (1840). From Cicero: "What is more sacred, what more inviolably hedged about by every kind of sanctity, than the home of every individual citizen? . . . [I]t is a sanctuary so holy in the eyes of all, that it were sacrilege to tear an owner therefrom." MARCUS TULLIUS CICERO, DE DOMA SUA xli. 109 (N.H. Watts ed. & trans. 1923). And from Hammurabi: "If a man makes a breach in a house, they shall put him to death in front of that breach and they shall thrust him therein." CODE OF HAMMURABI art. 21 (Robert Francis Harper ed. & trans., 2d ed. 1904) (ca. 1750 B.C.E.).

183. Frances E. Olsen, *The Family and the Market: A Study of Ideology and Legal Reform*, 96 HARV. L. REV. 1497, 1499 (1983) (citation and internal quotation marks omitted).

184. *See, e.g.*, L. FRANK BAUM, THE WONDERFUL WIZARD OF OZ 45 (1900) ("There is no place like home.").

185. *See, e.g.*, GLADIATOR 00:15:25–33 (DreamWorks Pictures 2000) (Emperor Marcus Aurelius: "How can I reward Rome's greatest general?" Maximus: "Let me go home."); THE LORD OF THE RINGS: THE TWO TOWERS 02:21:39–22:17 (New Line Cinema 2002) (Treebeard: "You are young and brave, Master Merry. But your part in this tale is over. Go back to your home." Pippin: "Maybe Treebeard's right. We don't belong here, Merry. It's too big for us. What can we do in the end? We've got the Shire. Maybe we should go home.").

a haven. All citizens "wish at some point to draw a line, to pull the shades, and to turn inward . . . [in order] to contemplate [their] own thoughts and feelings."[188] Since privacy is "[a]t the very core" of what the Fourth Amendment seeks to protect, and the home is the epitome of privacy in our nation, it is a vitally important point that current Fourth Amendment jurisprudence steadfastly protects it.[189] The Court has used the reasonable expectation of privacy test to ensure continued protection of the home and the privacy interests it embodies, even in the face of modern technologies like electronic tracking and infrared surveillance. Cases like *Karo* and *Kyllo* therefore demonstrate two instances in which the reasonable expectation of privacy test has successfully protected citizens' Fourth Amendment privacy interests. Even some of the commentators who have been most critical of the reasonable expectation of privacy test would seem to agree with this point. For instance, Professor Orin Kerr, though clearly critical of *Katz*, acknowledges that "an expectation of privacy becomes 'reasonable' . . . when it is backed by a right to exclude borrowed from real property," which includes a citizen's "reasonable expectation of privacy in his home."[190]

2. The Third-Party Doctrine: Societal Expectations and Effective Law Enforcement

Most commentators critical of the reasonable expectation of privacy test would not seriously contest that the Court has gone to great lengths to protect privacy interests in the home. Rather, commentators' worries lie largely in their belief that the reasonable expectation of privacy test fails to protect expectations of privacy outside the home environment. In particular, many commentators express great concern about the Court's application of third-party

186. *See, e.g.*, Vill. of Belle Terre v. Boraas, 416 U.S. 1, 9 (1974) (holding that it is constitutional for towns to pass zoning codes that aim "to lay out zones where family values, youth values, and the blessings of quiet seclusion and clean air make the area a sanctuary for people").

187. *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 158 & cmt. h (1965) (recognizing unauthorized entry into a home as tortious).

188. PRIVACY, *supra* note 182, at xiv.

189. *See supra* notes 177–78 and accompanying text; *see also* Wolf v. Colorado, 338 U.S. 25, 27 (1949) ("The security of one's privacy against arbitrary intrusion by the police—*which is at the core of the Fourth Amendment*—is basic to a free society." (emphasis added)).

190. Kerr, *supra* note 6, at 809–10; *see also* Katz & Mazzone, *supra* note 7, at 373 ("[T]he Court's focus on the warrant requirement and the requirement that exigency support warrantless searches [has] faded *except in the context of home searches*." (emphasis added) (internal citation omitted)); Maclin, *supra* note 7, at 116–18 (arguing that *Kyllo* and future cases will limit *Katz*'s application to *just the home*).

doctrine in its Fourth Amendment jurisprudence.[191] Though these commentators are correct that *Katz* offers less protection to privacy interests outside the home, this lower level of protection is not due to deficiencies in the reasonable expectation of privacy test. Rather, this lesser level of protection is due to a combination of long-standing precedent that predates *Katz*, society's actual expectations, and the needs of balancing private citizens' rights with those of efficient and effective law enforcement.

The Court's rulings in *United States v. White*[192] and *Smith v. Maryland*[193] received particular criticism from commentators for the manner in which they apply third-party doctrine to the reasonable expectation of privacy test.[194] In *White*, the Court held that no reasonable expectation of existed, and thus no search occurred, when an undercover government agent wore a wire and recorded conversations with the defendant for later use at trial.[195] Using similar reasoning, the Court in *Smith* concluded that citizens do not hold a reasonable expectation in the telephone numbers they dial because "[a]ll subscribers realize . . . that 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."[196]

The holdings of both *White* and *Smith* rested on the principle, well established before the Court ruled on *Katz*,[197] that once a citizen

191. *See, e.g.*, Henderson, *supra* note 158, at 511 ("'[T]hird party doctrine' must be strictly construed if the Fourth Amendment is to meaningfully limit government intrusions."); Swire, *supra* note 167, at 907–08 (arguing that cases like *Smith v. Maryland* have created a "narrow scope of the 'reasonable expectation of privacy' test"); Tomkovicz, *supra* note 157, at 359 (criticizing third-party doctrine's assumption "that a person suffers no violation or deprivation of confidentiality or secrecy if information about her life has been perceived or acquired because of the person's choice to reveal or expose that information"); Weaver, *supra* note 6, at 1193–94 (noting that since electronic communications and cloud computing are voluntarily conveyed to third parties (i.e., ISPs), the Court's rulings in cases like *Smith v. Maryland* could indicate that such actions are not protected by the reasonable expectation of privacy test); Lawless, *supra* note 167 (criticizing third-party doctrine for permitting warrantless searches of Internet users' search queries); *see also supra* Part III.A.

192. United States v. White, 401 U.S. 745 (1971) (plurality opinion); *see supra* Part III.A.

193. Smith v. Maryland, 442 U.S. 735 (1979); *see supra* Part III.A.

194. *See, e.g.*, Maclin, *supra* note 7, at 75–78 ("[T]he protective shield of *Katz* was just as ineffective in *Smith* as it was in *White*.").

195. *White*, 401 U.S. at 749–51.

196. *Smith*, 442 U.S. at 742.

197. *See* Hoffa v. United States, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to

discloses information to a third party or the public, that citizen assumes the risk of that information coming to the attention of law enforcement.[198] Several commentators criticized the Court for allowing this third-party doctrine to severely "limit" the reach of the reasonable expectation of privacy test.[199] "Limit" is a relative term in this context. Undoubtedly, if the Court were to do away with third-party doctrine, a much greater range of actions and locations would be protected by the Fourth Amendment. But such a ruling would be inconsistent with both the holding of *Katz* itself and the societal expectations the reasonable expectation of privacy test purports to represent.

On a most basic level, the third-party doctrine's application to the reasonable expectation of privacy test makes intrinsic sense. As one commentator aptly put it, "How can someone have a 'reasonable expectation of privacy' in information shared with the public?"[200] Language right out of the Court's opinion in *Katz* affirms this proposition: "What a person knowingly *exposes to the public*, even in his own home or office, is not a subject of Fourth Amendment protection."[201] Even Professor Tomkovicz, who is critical of third-party doctrine, admitted that this logic is persuasive: "The government does not intrude on core Fourth Amendment privacy values by perceiving what a person chooses to reveal or by receiving what an individual chooses to convey."[202] Put simply, it is unreasonable to expect information revealed to the public to remain private. A test based on the *reasonable* expectations of society simply cannot accord such information a legally recognized expectation of privacy.

On a more practical level, it is important to keep in mind that for every expansion of Fourth Amendment protection, another restriction is placed upon the methods law enforcement officers can use to keep us safe. To a point, of course, this is a good thing—the fundamental

---

whom he voluntarily confides his wrongdoing will not reveal it."); Lopez v. United States, 373 U.S. 427, 439 (1963) ("We think the risk that petitioner took in offering a bribe to [the law enforcement agent] fairly included the risk that the offer would be accurately reproduced in court, whether by faultless memory or mechanical recording.").

198. *White*, 401 U.S. at 752 ("Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police."); *Smith*, 442 U.S. at 743-44 ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); *see supra* Part III.A.

199. *See supra* note 195.

200. Sklansky, *supra* note 171, at 202.

201. Katz v. United States, 389 U.S. 347, 351 (1967) (emphasis added).

202. Tomkovicz, *supra* note 157, at 359–60.

purpose of the Fourth Amendment is to protect citizens from unreasonable governmental intrusion into their private and personal lives.[203] But there is also a point at which expansion of Fourth Amendment protection would begin to inhibit law enforcement too much. Achieving the proper balance between effective law enforcement and citizens' Fourth Amendment rights is perhaps the American legal system's greatest tug of war. As Professor Orin Kerr rightly pointed out, the goal of Fourth Amendment jurisprudence is to achieve

> a workable and sensible balance between law enforcement needs and privacy interests. The law should allow the government to investigate crime effectively, . . . [but] must [also] limit the power of government, in order to protect privacy and civil liberties against excessive government snooping.[204]

The Court's application of third-party doctrine has, for the most part,[205] done a good job of striking this balance.

The most significant law enforcement technique that third-party doctrine preserves is the use of informants. As Judge Learned Hand once observed, "[c]ourts have countenanced the use of informers from time immemorial; in cases of conspiracy, or in other cases when the crime consists of preparing for another crime, it is usually necessary to rely upon them or upon accomplices because the criminals will almost certainly proceed covertly."[206] Chief Justice Warren once expounded upon the importance of undercover operatives to effective law enforcement:

> There are some situations where the law could not adequately be enforced without the employment of some guile or misrepresentation of identity. A law enforcement officer performing his official duties cannot be required always to be in

---

203. This is evident from the text of the amendment:

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

U.S. CONST. amend. IV.

204. Kerr, *supra* note 6, at 861.

205. While the reasonable expectation of privacy test adequately protects citizens' Fourth Amendment privacy interests, there have been some questionable applications of third-party doctrine in the years since *Katz*. This issue is explored below in Part V.

206. United States v. Dennis, 183 F.2d 201, 224 (2d Cir. 1950) (citing several Supreme Court decisions).

> uniform or to wear his badge of authority on the lapel of his civilian clothing. Nor need he be required in all situations to proclaim himself an arm of the law. It blinks the realities of sophisticated, modern-day criminal activity and legitimate law enforcement practices to argue the contrary.[207]

Chief Justice Warren's assessment is particularly poignant against today's backdrop of modern technology and the security threats our country currently faces. As one commentator aptly put it, "constitutional restraint on police investigation could become even more crippling if police are locked into using primitive surveillance devices, while criminals or terrorists are left free to take advantage of emerging technologies to evade, or even surveil, the government officials trying to stop them."[208]

Undercover informants help police catch dangerous criminals. Had the Court not upheld third-party doctrine in *White*, this invaluable[209] crime fighting technique would have been rendered effectively useless. Police would need probable cause to employ an undercover agent. But in most cases police would not have such probable cause until they were reasonably certain that the suspect was guilty. This raises two issues. First, achieving probable cause may be next to impossible in some cases without inside information—information that can only be obtained with a secret informant. More importantly, if police are reasonably certain that a suspect is guilty, they can just arrest him. As such, by the time they would have enough information to legally employ an informant, the informant would not be needed![210] Law enforcement efforts would be severely hampered if police could never use undercover agents. The Court has noted that such "practical realities" must be taken into account when answering Fourth Amendment questions.[211]

As the example of undercover agents illustrates, third-party doctrine's restriction of citizens' reasonable expectations of privacy is necessary. In an ideal world, all citizens would be free from secret government surveillance at all times. But it is simply not possible to

---

207. Hoffa v. United States, 385 U.S. 293, 315 (1966) (Warren, C.J., dissenting).

208. Blitz, *supra* note 157, at 1413.

209. The Supreme Court has recognized "that the informer is a vital part of society's defensive arsenal." McCray v. Illinois, 386 U.S. 300, 307 (1967) (quoting State v. Burnett, 201 A.2d 39, 44 (N.J. 1964) (opinion of Weintraub, C.J.)).

210. KAMISAR ET AL., *supra* note 72, at 477.

211. Wyoming v. Houghton, 526 U.S. 295, 306 (1999) (holding that police officers with probable cause to search a car may inspect passengers' belongings found in the car if those objects are capable of concealing the object of the search).

achieve such a utopian ideal while maintaining adequate levels of effective law enforcement and national security. As one commentator stated the argument, "society can afford to erect strong privacy protections around the home and other private places only because police can begin their investigation outside of such private areas and gather the evidence necessary to decide what intrusions into private areas are really essential."[212] This argument sums up a delicate issue quite well—if society wants staunch protection of its most private places, it must accept that the efficient and effective pursuit of law enforcement requires reduced levels of privacy outside those areas. As such, commentators are correct to point out that the Court's adherence to third-party doctrine in its Fourth Amendment jurisprudence has, in some ways, limited the amount of citizen privacy the reasonable expectation of privacy test is able to protect. But such limits are necessary to strike an adequate balance between citizens' rights and effective law enforcement.

Also, it is not as if there are no safeguards in place to restrain overly zealous law enforcement. Officers obtaining evidence in violation of the Fourth Amendment pay the ultimate price—that evidence can be deemed inadmissible in a criminal trial as the "fruit of the poisonous tree."[213] And even when a suspect speaks with a secret government informant, the scope of consent that the suspect has granted restricts the informant. As such, an undercover agent willingly admitted into one's home or office cannot, for instance, rummage through drawers when that person steps into another room.[214] The Court has also pointed out that "practical considerations"—such as "limited police resources and community hostility [to overly invasive tactics]—seem

212. Blitz, *supra* note 157, at 1413.

213. Nardone v. United States, 308 U.S. 338, 341 (1939); *see also* Weeks v. United States, 232 U.S. 383 (1914) (holding that evidence obtained during an unconstitutional search is suppressed in federal criminal trials); Mapp v. Ohio, 367 U.S. 643 (1961) (holding that the Fourteenth Amendment requires all states to abide by the *Weeks* suppression rule); Illinois v. Rodriguez, 497 U.S. 177, 183 (1990) ("What [the defendant] is assured by the trial right of the exclusionary rule, where it applies, is that no evidence seized in violation of the Fourth Amendment will be introduced at his trial unless he consents.").

214. Gouled v. United States, 255 U.S. 298, 305–06 (1921); *see also* KAMISAR ET AL., *supra* note 72, at 461 (quoting Florida v. Jimeno, 500 U.S. 248, 251–52 (1991) ("The standard for measuring the scope of a suspect's consent . . . [under the Fourth Amendment is] that of 'objective' reasonableness—what would the typical reasonable person have understood by the exchange between the officer and the suspect? . . . It is very likely unreasonable to think that a suspect, by consenting to the search of his trunk, has agreed to the breaking open of a locked briefcase within the trunk, but it is otherwise with respect to a closed paper bag.")).

likely to inhibit . . . proliferation" of unconstitutional search practices.[215] Other procedural safeguards exist as well, such as the rules of evidence, placing the burden of proof on the government, juries, and laws enacted by legislatures, both state and federal. Such protections help ensure that third-party doctrine does not encroach onto citizens' Fourth Amendment privacy interests.

3. The Third-Party Doctrine and Privacy in Public Areas

While the Court's application of third-party doctrine in the Fourth Amendment context reduces citizens' public privacy in some circumstances, the Court's jurisprudence also indicates that third-party doctrine will not overrun all privacy interests outside the home. For instance, and contrary to the apparent fears of some commentators, the Court has made clear that it would not put up with dragnet-type surveillance of the American public—a *1984*-like dystopia[216] will not be making an appearance in American society any time soon.[217] Such invasions of privacy are not, and never will be, permitted by the Court's Fourth Amendment jurisprudence.

Some commentators' greatest fears lie in the potential invasions of privacy posed by technologies like GPS tracking and video

215. Illinois v. Lidster, 540 U.S. 419, 426 (2002).

216. GEORGE ORWELL, 1984 (1949).

217. *See, e.g.*, Renee McDonald Hutchins, *Tied up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 411 (2007) ("Though the necessities of modern life may at times require the disclosure of discrete portions of our daily routine to the handful of private parties that provide us with services, it is unlikely most Americans would sanction pervasive monitoring by our government. If we are to avoid the Orwellian predictions of some conspiracy theorists, we must find meaningful ways to limit the government's ability to keep tabs on us. The Fourth Amendment is our first line of defense."); Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583, 600 (1989) (arguing that the Court's *Smith* opinion "smacks of Orwell's Big Brother, protection from which is the essence of the fourth amendment"); Weaver, *supra* note 6, at 1135 ("Today, eavesdropping and other surveillance technologies have gone high tech and created Orwellian possibilities for snooping."). For what it is worth, the author rolls his eyes whenever a commentator puts forth such cliché *1984* references. Even if the Fourth Amendment has been reduced to as much of an irrelevancy as some commentators make it out to be (which this Note argues is not the case), every other right guaranteed by the Bill of Rights would also have to be whittled away to similar irrelevancy before our society would even approach that of Orwell's dystopia. And Justice Breyer, at least, would seem to agree. *See* Transcript of Oral Argument at 13, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf (referring to respondent's reference to *1984* as overly dramatizing).

surveillance.[218] Today's "GPS-enabled surveillance allows a single person to remotely (and simultaneously) monitor the movements of one or more individuals for limitless periods or to determine their precise location at any moment,"[219] and video surveillance could one day give the government the ability to virtually stop anyone on the street by simply pushing the pause button, "enhancing or magnifying detail, and electronically matching aspects of each person's appearance against biometric or other databases."[220] While modern technology has indisputably made such government actions possible, the Fourth Amendment remains up to the task of defending citizens from unwarranted government intrusions. Even before the Court's recent decision in *Jones*, there was abundant Supreme Court jurisprudence that indicates the High Court would not permit such extreme invasions of privacy.

In *Knotts*,[221] a case that received significant criticism for its allowance of warrantless electronic "beeper" surveillance of a car travelling on public highways,[222] the Court limited its holding in several ways that will likely have significant impact on future Fourth Amendment decisions. At least one commentator pointed out that the Court, as it often does, limited its holding to just the beeper technology at issue in the case.[223] As such, *Knotts* is not controlling precedent over other cases involving modern technology. The Court made this fact crystal clear in *Jones*.[224] Further, the now almost arcane beeper technology at issue in *Knotts* is hardly similar to much more modern technologies like GPS. "[T]he appropriate constitutional treatment of GPS- [and video-] enhanced surveillance is not tied up in

218. While the Court's recent decision in *Jones* dealt with GPS technology, academic commentary and speculation about GPS technology and its impact on the Fourth Amendment is still very relevant because *Jones* was decided on the very narrow ground that the government obtained information by trespassing upon a constitutionally protected area. *See* United States v. Jones, 132 S. Ct. 945 (2012); *supra* Part III.E (discussing *Jones*). As such, *Jones* left open several questions about the constitutionality of searches utilizing GPS technology. But such debates will likely be resolved in favor of citizen privacy interests. *See infra* Part IV.B.4 (analyzing *Jones*).

219. Hutchins, *supra* note 217, at 413.

220. Blitz, *supra* note 157, at 1356.

221. United States v. Knotts, 460 U.S. 276, 277 (1983).

222. *See, e.g.*, Maclin, *supra* note 7, at 83 ("[T]he result and reasoning of *United States v. Knotts* reveals the insignificance of *Katz's* proclamation that the Fourth Amendment's reach 'cannot turn upon the presence or absence of a physical intrusion into any given enclosure.'").

223. Hutchins, *supra* note 217, at 457.

224. *See Jones*, 132 S. Ct. at 952 (noting that *Knotts* was not "relevant" to the Jones situation.).

Knotts because, as a factual matter, beeper and GPS technology are fundamentally different in terms of the quantity of information revealed by the science."[225] And, as Justice Sotomayor recently pointed out, GPS technology is highly intrusive, revealing much more information than the beepers at issue in *Knotts* could have ever uncovered.[226]

Perhaps most importantly, the Court in *Knotts* strongly suggested that "dragnet-type" government surveillance practices would not be upheld under the Fourth Amendment.[227] In response to the defendant's argument that allowing unwarranted beeper surveillance would allow the government to conduct "twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision[,]" the Court made clear that such surveillance was not at issue in *Knotts* and suggested that its holding would have been quite different under those circumstances: "[I]f such dragnet-type law enforcement practices as [the defendant] envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[228] This language suggests that the Court would not, as some commentators fear,[229] stand for the government placing all of this nation's citizenry under constant surveillance.

Just a few years after *Knotts*, the Court further suggested that dragnet government surveillance is unconstitutional. In *Dow Chemical*,[230] the Court upheld the EPA's warrantless use of high-tech cameras during a flyover of a chemical plant to inspect for violations. Despite this holding, the Court included noteworthy limiting language in its opinion that will likely prove significant in future Fourth Amendment decisions. The Court noted that the use of "highly sophisticated surveillance equipment . . . such as satellite technology, might be constitutionally proscribed absent a warrant."[231] It went on to explain that, in this case, the photographs taken by the EPA were

225. Hutchins, *supra* note 217, at 457.

226. *See Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

227. *Knotts*, 460 U.S. at 284.

228. *Id.*

229. *See, e.g.*, Blitz, *supra* note 157, at 1356 (arguing that "the absence of . . . constitutional limitation [of video surveillance] seems to leave authorities free to engage in a variant of the dragnet searches that the Fourth Amendment was clearly intended to prevent").

230. Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

231. *Id.* at 238.

> not so revealing of intimate details as to raise constitutional concerns. Although they undoubtedly give [the] EPA more detailed information than naked-eye views, they remain limited to an outline of the facility's buildings and equipment.[232]

The Court further emphasized the lack of intimate details revealed by the EPA's surveillance:

> No objects as small as . . . a class ring, for example, are recognizable, nor are there any identifiable human faces or secret documents captured in such a fashion as to implicate more serious privacy concerns. Fourth Amendment cases must be decided on the facts of each case, not by extravagant generalizations.[233]

The Court's strong emphasis on the revelation (or lack thereof) of intimate details indicates that it would not accept wholesale the extreme level of detail that could potentially be revealed about the everyday lives of American citizens by technologies like GPS and video surveillance. As one commentator argued, the language cited above from *Dow Chemical* suggests that the Court has incorporated an "intrusiveness inquiry" into the reasonable expectation of privacy test, the result of which is that the "Court's existing framework . . . provides a meaningful safeguard against law enforcement's unfettered use of GPS-enhanced tracking," and presumably also video surveillance.[234] Though the Court's decisions that have followed *Dow Chemical* do not seem to use this inquiry explicitly, intrusiveness certainly does seem to play a role in the Court's analysis. The discussion of the lack of "intimate details" revealed by the camera in *Dow Chemical* would have been unnecessary otherwise.[235] Further, this past term in *Jones*, Justice Sotomayor noted that in future GPS surveillance cases she would look to the intrusive nature of GPS technology when determining citizens' reasonable expectations of privacy.[236]

The Court in *Dow Chemical* also pointed out that the property at issue was a business, not a home. The owners of businesses cannot reasonably expect the same level of privacy as homeowners because, unlike homes, businesses are not "free from any inspections."[237]

---

232. *Id.*

233. *Id.* at 238 n.5.

234. Hutchins, *supra* note 217, at 458, 460.

235. *Dow Chem.*, 476 U.S. at 238.

236. United States v. Jones, 132 S. Ct. 945, 955–56 (2012) (Sotomayor, J., concurring).

237. *Dow Chem.*, 476 U.S. at 238.

Finally, in *Kyllo*,[238] the Court explicitly recognized the dangers posed to citizen privacy by modern technology and made clear its dedication to preventing unwarranted invasions of privacy. Justice Scalia's majority opinion in *Kyllo* eloquently rebutted the argument that the thermal imager at issue only picked up "off-the-wall" information about the defendant's house, and thus did not constitute a Fourth Amendment search:

> But just as a thermal imager captures only heat emanating from a house, so also a powerful directional microphone picks up only sound emanating from a house—and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house. We rejected such a mechanical interpretation of the Fourth Amendment in *Katz*, where the eavesdropping device picked up only sound waves that reached the exterior of the phone booth. Reversing that approach would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home. While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.[239]

Justice Scalia makes abundantly clear that the Court is well aware of the potential dangers modern technology poses to citizens' Fourth Amendment rights. This knowledge, combined with the fact that *Kyllo* was unquestionably a victory for Fourth Amendment rights, indicates that the current Court is more than prepared to use *Katz's* reasonable expectation of privacy test to shield citizens' privacy interests from the prying eyes of potential Big Brothers.

4. The Impact of *Jones* on Fourth Amendment Jurisprudence

After more than a ten-year hiatus from deciding a Fourth Amendment case involving technology,[240] the Court handed down a Fourth Amendment Decision involving GPS surveillance, *United States v. Jones*,[241] in January 2012. Not surprisingly, in the short time between the Court's decision and the writing of this Note, several commentators have already begun to criticize the opinion. Other

238. Kyllo v. United States, 533 U.S. 27 (2001).

239. *Id.* at 35–36.

240. As noted above, *see supra* note 165, in 2010 the Court dealt with a Fourth Amendment case that involved text messaging, but sidestepped the technology issue and relied on already established principles of Fourth Amendment and employment law. City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

241. United States v. Jones, 132 S. Ct. 945 (2012).

commentators, however, have had positive reactions. This section summarizes the views of several of these commentators and also provides an analysis of *Jones*. It argues that *Jones* provides citizens with much reason to believe that the Court intends to wield the reasonable expectation of privacy test as a shield for privacy interests in future Fourth Amendment and technology cases.

As with many of the Court's other Fourth Amendment and technology decisions, several commentators have been highly critical of the holding in *Jones*. Professor Kerr noted that the case raises several new Fourth Amendment questions, including "[w]hat kind of 'trespass' counts for purposes of [the majority's trespassory] test?"[242] Kerr is critical of both Justices Scalia and Alito for not fully explaining the tests they used to determine the appropriate outcome of *Jones*.[243] This lack of clarity, argued Kerr, "make[s] the decision a Rorschach test."[244] Tom Goldstein, a well-known appellate litigator and the co-founder of SCOTUSblog, argued that *Jones* is "less of a pro-privacy ruling than many people initially thought."[245] Goldstein criticizes the decision in *Jones* for failing to hold that installation of GPS tracking devices and short-term GPS monitoring are searches.[246] In what was possibly the harshest view of *Jones* expressed in the weeks following its release, Goldstein noted:

> I don't see in *Jones* anything that remotely resembles a working majority on the Court for the conclusion that technological advances require the adoption of a new or broader conception of personal privacy. And I think it signals to the government that

242. Orin Kerr, *Three Questions Raised By The Trespass Test in* United States v. Jones, VOLOKH CONSPIRACY (Jan. 23, 2012, 6:57 PM), http://volokh.com/2012/01/23/three-questions-raised-by-the-trespass-test-in-united-states-v-jones/.

243. Orin Kerr, *Why* United States v. Jones *is Subject to So Many Different Interpretations*, VOLOKH CONSPIRACY (Jan. 30, 2012, 4:59 PM), http://volokh.com/2012/01/30/why-united-states-v-jones-is-subject-to-so-many-different-interpretations/ ("Justice Scalia creates a new test for Fourth Amendment searches without being fully candid that he's doing something quite new. . . . Scalia is so dismissive of Alito's critique that it's hard to know why Scalia sees Alito's questions as so obviously answered. . . . Justice Alito spends only a single paragraph of his 14-page opinion explaining how he would resolve the *Jones* case. . . . And in that one paragraph, Alito is surprisingly unclear as to what he is doing.").

244. *Id.*

245. Tom Goldstein, *Why* Jones *is Still Less of a Pro-Privacy Decision than Most Thought*, SCOTUSBLOG (Jan. 30, 2012, 10:53 AM), http://www.scotusblog.com/2012/01/why-jones-is-still-less-of-a-pro-privacy-decision-than-most-thought/.

246. *Id.*

> in many respects its investigatory efforts are not subject to the Fourth Amendment.[247]

Another commentator noted that "the majority holding will soon be obsolete, because police don't need to physically attach a tracker to your car to use GPS tracking."[248] And yet another criticized the Court for leaving "unsettled the question of how much protection one may expect from the Fourth Amendment in the digital age."[249]

Other commentators have been much friendlier to *Jones*. Professor Sherry F. Colb expressed that she felt "optimistic about the future of the Fourth Amendment" after reading *Jones*.[250] She noted that while Justices Scalia and Alito disagreed on the appropriate test to apply in the case, they both "endorse the 'reasonable expectation of privacy' test."[251] Professor Colb rightly pointed out that "[t]he fact that Justices Scalia and Alito are battling over who best protects the privacy interests of the defendant should be quite exciting to fans of constitutional privacy."[252] Other commentators seem to share Colb's optimism. One noted that *Jones* indicates that "a majority of the justices are prepared to apply broad privacy principles to bring the Fourth Amendment's ban on unreasonable searches into the digital age."[253] This commentator also cited with approval the expressions of Justices Alito, Ginsburg, Breyer, Kagan, and Sotomayor demonstrating "discomfort with the government's use of or access to various modern technologies."[254] Washington lawyer Andrew Pincus, who filed a brief on Jones's behalf, called the Court's decision a

247. *Id.*

248. Margot Kaminski, *Reactions to* US v. Jones, INFO. SOC'Y PROJECT YALE L. SCH. (Jan. 24, 2012), http://yaleisp.org/2012/01/reactions-to-us-v-jones/.

249. Mike Sacks, *Warrantless GPS Tracking Unconstitutional, Supreme Court Rules*, HUFFINGTON POST (Jan. 23, 2012, 1:24 PM), http://www.huffingtonpost.com/2012/01/23/warrantless-gps-tracking-_n_1224000.html.

250. Sherry F. Colb, *The Supreme Court Decides the GPS Case,* United States v. Jones*, and the Fourth Amendment Evolves*, VERDICT JUSTIA (Feb. 15, 2012), http://verdict.justia.com/2012/02/15/the-supreme-court-decides-the-gps-case-united-states-v-jones-and-the-fourth-amendment-evolves-2.

251. *Id.*

252. *Id.*

253. Adam Liptak, *Justices Reject GPS Tracking in a Drug Case*, N.Y. TIMES, Jan. 24, 2012, at A1. This article also quotes Walter Dellinger, one of Jones's attorneys, calling the decision "a signal event in Fourth Amendment history." *Id.*

254. *Id.* at A3.

"landmark ruling in applying the Fourth Amendment's protections to advances in surveillance technology."[255]

It should come as no surprise that this Note agrees with those commentators with optimistic outlooks on the Court's ruling in *Jones*. While commentators may be correct that the configuration of opinions in *Jones* is somewhat confusing, careful analysis of the Justices' views paints a bright picture for both the future of the reasonable expectation of privacy test and Fourth Amendment jurisprudence in general.

Let us begin with the majority opinion. Admittedly, the *Jones* majority did not rest its ruling on *Katz* and the reasonable expectation of privacy test. But the opinion still abounds with reassuring language about both the Court's continued dedication to protecting privacy rights and the reasonable expectation of privacy test's continued viability. The Court began by noting that "our law holds the property of every man so sacred, that no man can set his foot upon his neighbour's [personal property] without his leave . . . ."[256] Thus, the majority established from the start that citizens' interest in being free from intrusions upon their personal property was a core issue in the case. This interest is at the core of the privacy rights protected by the Fourth Amendment[257] and was unequivocally protected by the Court:

> [T]he Fourth Amendment . . . embod[ies] a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates. *Katz* did not repudiate that understanding . . . . By attaching the device to the Jeep [without a warrant], officers encroached on a protected area [and thus violated the Fourth Amendment].[258]

While this was undoubtedly a narrow holding,[259] the majority also made evident that it supported an expansive view of the Fourth Amendment. It noted that its trespassory analysis was not a

255. Robert Barnes, *Supreme Court: Warrants Needed in GPS Tracking*, WASH. POST (Jan. 23, 2012), http://www.washingtonpost.com/politics/supreme-court-warrants-needed-in-gps-tracking/2012/01/23/gIQAx7qGLQ_story.html.

256. United States v. Jones, 132 S. Ct. 945, 949 (2012) (quoting Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.) 817).

257. *See Jones*, 132 S. Ct. at 949; Brower v. County of Inyo, 489 U.S. 593, 596 (1989); Boyd v. United States, 116 U.S. 616, 626 (1886).

258. *Jones*, 132 S. Ct. at 950, 952 (quoting U.S. CONST. amend. IV).

259. As Justice Sotomayor noted in her concurrence, the majority's holding represented an "irreducible constitutional minimum," which "supplie[d] a narrow[] basis for decision." *Id.* at 955, 957 (Sotomayor, J., concurring).

substitution for, but rather an addition to, the reasonable expectation of privacy test.[260] As such, it criticized Justice Alito's concurring opinion for placing undue restrictions on the Fourth Amendment, "which would make *Katz* the *exclusive* test."[261] The Court noted that such an approach would pose "particularly vexing problems," including creating a Fourth Amendment jurisprudence that would fail to protect "that degree of privacy against government that existed when the Fourth Amendment was adopted."[262] Thus, the majority was clearly cognizant of the need to ensure that its ruling protected citizens' privacy. The Court also made clear that the reasonable expectation of privacy test remains the default test for when information is obtained in a non-trespassory fashion:

> Situations involving merely the transmission of electronic signals without trespass . . . *remain* subject to *Katz* analysis. . . . It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy . . . .[263]

The concurring opinions of Justices Sotomayor and Alito show even more promise for the protection of privacy interests. The most significant aspect of these opinions is that they both agree that long-term GPS surveillance violates citizens' reasonable expectations of privacy.[264] This agreement will likely be of the utmost importance in future technology cases because it means that a majority of the Court (Sotomayor, Alito, and the three justices who joined Alito—Ginsburg, Breyer, and Kagan) is prepared to hold that warrantless long-term GPS monitoring is unconstitutional under the reasonable expectation of privacy test. This would be a huge victory for privacy advocates and clearly demonstrates that the reasonable expectation of privacy

260. *Id.* at 952 (majority opinion) ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

261. *Id.* at 953.

262. *Id.* at 950, 953 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

263. *Id.* at 953–54; *see also* United States v. Cowan, 674 F.3d 947, 955 n.3 (8th Cir. 2012) ("The Supreme Court in *Jones* refused to overrule the *Katz* line of cases, stating that the cases are still good law with regard to whether the government has violated an individual's reasonable expectation of privacy, but those cases do not address the second, 'the common-law trespassory,' prong of the Fourth Amendment analysis." (citing *Jones*, 132 S. Ct. at 951–53)).

264. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."); *id.* at 955 (Sotomayor, J., concurring) ("I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'").

test is capable of protecting citizens' privacy from advancing technologies. Both opinions further recognize that citizens should not have to expect a lower level of privacy simply because technology has made it easier for the government to encroach upon privacy interests.[265] As such, contrary to Tom Goldstein's view, there actually does seem to be a "working majority on the Court" prepared to adopt "a new or broader conception of personal privacy."[266]

This is not to say that the *Jones* opinion raised no new questions. Most significant of these is the constitutionality of warrantless *short-term* GPS surveillance. Justice Alito and the three justices joining him clearly think it would be constitutional.[267] And, based on her concurring opinion, Justice Sotomayor would likely hold it to be unconstitutional.[268] The view of the remaining four justices in the majority remains somewhat unclear, though they may have suggested agreement with Justice Sotomayor when the majority opined that "[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy."[269] But the uncertainty raised by this and other questions posed by *Jones* is hardly reason to criticize the opinion. The Court frequently resolves cases on narrow grounds, declining to "rush forward" and resolve issues that are not yet before it.[270]

The important lesson from *Jones* is twofold: (1) *all nine justices* voted in favor of protecting the defendant's Fourth Amendment rights from a warrantless GPS search; and (2) a majority of the Court

265. *See id.* at 964 (Alito, J., concurring) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."); *id.* at 956 (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms. . . . I do not regard as dispositive the fact that the government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques.").

266. Goldstein, *supra* note 245 ("So I don't see in *Jones* anything that remotely resembles a working majority on the Court for the conclusion that technological advances require the adoption of a new or broader conception of personal privacy."). Considering the opinions, Goldstein's observation is somewhat perplexing.

267. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) ("[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable.").

268. *See id.* at 955–56 (Sotomayor, J., concurring) (questioning whether, due to the extremely intrusive nature of GPS surveillance, warrantless use of such a surveillance technique would ever be constitutional).

269. *Id.* at 954 (majority opinion).

270. *Id.*

believes that long-term GPS surveillance is contrary to society's reasonable expectations of privacy. These two things represent a significant victory for privacy advocates. That the Court is arguing about how best to protect privacy—as opposed to whether to protect it at all—bodes quite well for the proposition that *Katz* and the reasonable expectation of privacy test are up to the task of protecting citizens' privacy interests from advancing technology.[271]

C. The Reasonable Expectation of Privacy Test in Lower Courts

The Supreme Court's jurisprudence is not the only place we can find evidence of the reasonable expectation of privacy test's continued viability in the technology context. Many lower courts have also applied the reasonable expectation of privacy test and the Court's Fourth Amendment case law in a manner that successfully protects citizens' privacy interests from modern technology. The areas of video surveillance and e-mail provide two telling examples.

1. Video Surveillance

Several federal circuit courts have held that citizens have a reasonable expectation of privacy against visual surveillance in private areas like homes and offices. The Seventh Circuit was the first to address this issue in detail. In *United States v. Torres*,[272] federal agents, after obtaining the authorization of a magistrate as required under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"),[273] installed television cameras in the apartment of several men suspected to be members of a notoriously violent Puerto Rican independence group.[274] The cameras revealed that the men were building bombs in the apartment. The agents used this revelation to obtain a search warrant for the premises, and the men were ultimately charged with seditious conspiracy.[275]

The Seventh Circuit, per Judge Posner, upheld the video surveillance of the apartment. It made abundantly clear, however, that the court viewed video surveillance differently from other, more traditional forms of surveillance. The opinion noted that if the police had not obtained authorization from a federal judge in accordance with Title III, the use of video surveillance would have violated the Fourth Amendment.[276] The holding in *Torres* was largely based on

271. *See* Colb, *supra* note 250.

272. United States v. Torres, 751 F.2d 875 (7th Cir. 1984).

273. 18 U.S.C. §§ 2510–2522 (2006).

274. *Torres*, 751 F.2d at 876–77.

275. *Id.* at 876.

276. *See id.* at 882–83, 885 ("[I]n declining to hold television surveillance unconstitutional per se [the Seventh Circuit does] not suggest that the Constitution must be interpreted to allow it to be used as generally as

the "indiscriminate" and "intrusive" nature of video surveillance, which the Seventh Circuit believed posed an even greater threat to citizens' privacy than physical searches: "We think it also unarguable that television surveillance is exceedingly intrusive, especially in combination (as here) with audio surveillance, and inherently indiscriminate, and that it could be grossly abused—to eliminate personal privacy as understood in modern Western nations."[277] The Seventh Circuit's concern with the privacy issues raised by video surveillance is certainly consistent with *Katz* and its reasonable expectation of privacy test. Thus, although it did not specifically reference the reasonable expectation of privacy test, it appears that the Seventh Circuit would have held the use of warrantless video surveillance unconstitutional as inconsistent with society's expectations of privacy.[278]

The Seventh Circuit's recognition of the highly intrusive nature of video surveillance is important for another reason as well. Some surveillance technologies reveal so much information that, in order to accurately determine whether a reasonable expectation of privacy has been violated, it may one day become necessary to consider not only whether surveillance occurred, but also the surveillance technique's

---

less intrusive techniques can be used. . . . [A] warrant for television surveillance that did not satisfy the four provisions of Title III that implement the Fourth Amendment's requirement of particularity would violate the Fourth Amendment.").

277. *Id.* at 882; *see also id.* at 887–88 (Cudahy, J., concurring) (explaining that Title III initially exempted electronic surveillance from its strict warrant requirements for national security purposes, but later repealed that exemption as part of the Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 ("FISA"), in order to protect citizens' reasonable expectations of privacy). FISA defines "electronic surveillance" as

> the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes . . . .

50 U.S.C. § 1801(f) (2006).

278. In his concurring opinion, Judge Cudahy noted that the court should "construe Title III to apply to video surveillance for domestic law enforcement investigations where the targets of the surveillance have a reasonable expectation of privacy." *Torres*, 751 F.2d at 894 (Cudahy, J., concurring); *see also* Blitz, *supra* note 157, at 1378 ("Judge Posner's decision [in *Torres*] subjected video surveillance within private homes or businesses to strict constitutional limits, intended to ensure that such surveillance takes place only when it is necessary.").

level of invasiveness. The Supreme Court seems well aware of this issue. Justice Sotomayor, for instance, noted in her *Jones* concurrence that she would account for the invasiveness of GPS surveillance in future cases when deciding whether such surveillance is contrary to society's reasonable expectations of privacy.[279] Such an intrusiveness inquiry would not be without Fourth Amendment precedent. In *Dow Chemical*,[280] the Court seemed to place great importance on the fact that the aerial surveillance at issue did not reveal "intimate details" and thus was not intrusive enough to raise a constitutional issue.[281] The Court has considered the degree of intrusiveness inherent in a search technique in several other Fourth Amendment cases as well.[282]

Since the Seventh Circuit's ruling in *Torres*, at least six other federal circuit courts have handed down similar opinions with regard to video surveillance.[283] The Ninth Circuit's decision in *United States*

279. *See* United States v. Jones, 132 S. Ct. 945, 955–56 (2012) (Sotomayor, J., concurring) ("In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . . I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements.").

280. Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

281. *Id.* at 238.

282. *See, e.g.*, Ybarra v. Illinois, 444 U.S. 85, 106 (1979) (Rehnquist, J., dissenting) ("[I]n judging the reasonableness of a search pursuant to a warrant, which search extends to persons present on the named premises, this Court should consider the *scope of the intrusion* as well as its justification." (emphasis added)); s*ee also* Bond v. United States, 529 U.S. 334, 337 (2000) (finding that officer's tactile search of a bus passenger's luggage violated the Fourth Amendment because "[p]hysically invasive inspection is simply more intrusive than purely visual inspection"); Wyoming v. Houghton, 526 U.S. 295, 303 (1999) (considering "the *degree of intrusiveness* upon personal privacy" caused by a police search of a defendant's motor vehicle when deciding the constitutionality of the search (emphasis added)); United States v. Place, 462 U.S. 696, 707 (1983) (deciding that although citizens have a reasonable expectation of privacy in their luggage, the warrantless use of drug dogs to sniff luggage does not violate the Fourth Amendment because a canine sniff "is much less intrusive than a typical search").

283. *See* Blitz, *supra* note 157, at 1378 n.154 ("Six other circuits have since [*Torres*] imposed the identical or nearly identical constraints on video surveillance and repeated the Seventh Circuit's warning that video surveillance can be incredibly destructive of privacy and must be carefully limited." (citing United States v. Williams, 124 F.3d 411, 416 (3d Cir. 1997); United States v. Falls, 34 F.3d 674, 680 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 1992); United States v. Mesa-Rincon, 911 F.2d 1433, 1438 (10th Cir. 1990); United

v. Nerber[284] is a notable example. Prior to a drug deal, police installed, without first obtaining a warrant, a camera in the defendants' hotel room and later attempted to use video from that camera as evidence at the defendants' trial. The Ninth Circuit held the video surveillance to be unconstitutional under the reasonable expectation of privacy test, noting that the "[d]efendants' expectation to be free from hidden video surveillance when alone in [their] hotel room was . . . objectively reasonable."[285] Like the Seventh Circuit, the *Nerber* court was troubled by the inherent intrusiveness of video surveillance:

> [T]he legitimacy of a person's *expectation of privacy* may depend on the nature of the intrusion . . . . "[E]very court considering the issue has noted [that] video surveillance can result in extraordinarily serious intrusions into personal privacy. . . . If such intrusions are ever permissible, they must be justified by an extraordinary showing of need."[286]

This language provides further support for the proposition that the intrusiveness of surveillance technology should be taken into account when determining what constitutes a reasonable expectation of privacy.

Cases like *Torres* and *Nerber* demonstrate that, at least as far as video surveillance is concerned, *Katz's* reasonable expectation of privacy test has succeeded in protecting citizens' Fourth Amendment privacy interests in the lower courts. Further, the reasonable expectation of privacy test has permitted lower courts to create a blueprint that the Supreme Court can use for dealing with intrusive surveillance technologies.

2. E-mail

Perhaps even more significant to today's society is the question of how the Fourth Amendment applies to searches of e-mail.[287] Eighty-

States v. Cuevas-Sanchez, 821 F.2d 248, 252 (5th Cir. 1987); United States v. Biasucci, 786 F.2d 504, 510 (2d Cir. 1986))).

284. United States v. Nerber, 222 F.3d 597 (9th Cir. 2000).

285. *Id.* at 605.

286. *Id.* at 603 (emphasis added) (quoting United States v. Koyomejian, 970 F.2d 536, 551 (9th Cir. 1992) (Kozinski, J., concurring)). The *Nerber* court also cited Judge Posner's opinion in *Torres*, 781 F.2d at 882, noting that "television surveillance is exceedingly intrusive . . . [and] could be grossly abused to eliminate personal privacy as understood in modern Western nations." *See Nerber*, 222 F.3d at 603–04.

287. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010) ("This question is one of grave import and enduring consequence, given the prominent role that email has assumed in modern communication."); *see also id.* at 286 ("Over the last decade, email has become 'so pervasive that some persons may consider [it] to be [an] essential means

five percent of American adults now use the Internet and, as access continues to become both cheaper and more widespread, this number can only be expected to grow.[288] With so many Americans using the Internet on a regular basis, electronic communications like e-mail are becoming citizens' preferred mode of communication.[289] As courts are beginning to recognize, "[e]-mail is almost equivalent to sending a letter via the mails."[290] In fact, the Supreme Court itself has recognized this similarity, albeit in a context outside the Fourth Amendment.[291] As such, commentators argue that e-mail ought to be afforded the same level of Fourth Amendment protection as regular mail.[292] Although the amount of case law is as of yet slim, several lower court opinions seem to agree with this analogy and have used *Katz's* reasonable expectation of privacy test to protect e-mail in a manner similar to that of regular mail.[293]

---

or necessary instrument[ ] for self-expression, even self-identification.'" (alteration in original) (quoting *City of Ontario v. Quon*, 130 S. Ct. 2619, 2630 (2010))).

288. *Demographics of Internet Users*, PEW RES. CENTER, http://www.pewinternet.org/Static-Pages/Trend-Data-(Adults)/Whos-Online.aspx (last visited Oct. 4, 2012).

289. *See, e.g.*, *Warshak*, 631 F.3d at 284 ("Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place.").

290. Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. Ct. 2001) (quoting United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997)).

291. Reno v. ACLU, 521 U.S. 844, 851 (1997) ("E-mail enables an individual to send an electronic message—generally akin to a note or letter—to another individual or to a group of addressees.").

292. *See, e.g.*, Ray, *supra* note 169, at 234 ("Courts have recognized that sending an e-mail message is essentially the equivalent of sending a letter through the mail. As such, an e-mail message should receive the same protection as a letter sent through the mail and should not be intercepted without a warrant.").

293. At least one commentator seems to disagree on this point. *See, e.g.*, *id.* at 210 ("[M]any courts have declined to find an expectation of privacy in e-mail or e-mail accounts."). But such commentators tend to point towards e-mail cases that are decided under well-established concepts of either third-party doctrine or employment law. *See, e.g.*, Rehberg v. Paulk, 598 F.3d 1268, 1281 (11th Cir. 2010) ("A person also loses a reasonable expectation of privacy in emails, *at least after the email is sent to and received by a third party.*" (emphasis added)); *Ray, supra* note 158, at 212 ("The Fourth Circuit has . . . found no reasonable expectation of privacy in e-mail messages sent over *an employer's* network." (emphasis added) (citing United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000))). While responding to all lower court holdings regarding the Fourth Amendment and e-mail is outside the scope of this Note, the author would argue that these cases were decided correctly under the Court's current Fourth Amendment jurisprudence. *See* City

Well-established Supreme Court jurisprudence holds that sealed mail may not be opened by the government absent probable cause and a warrant.[294] Since e-mail affords a level of security greater than that of normal mail, it would make sense to hold that e-mail retains an expectation of privacy at least as great as that which society places in other mail.[295] The holdings of several lower courts seem to indicate that this is indeed the trend.

In *United States v. Maxwell*,[296] a military court grappled with the warrantless search of an Air Force officer's e-mail account. The court held that evidence resulting from this search had to be suppressed because "the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant."[297] The court then "conclude[d] that under the circumstances here appellant possessed a reasonable expectation of privacy . . . in the e-mail messages that he sent and/or received on AOL."[298] In reaching this conclusion, the court noted that e-mail communication is not unlike other forms of modern communication: "For example, if a sender of first-class mail seals an envelope and addresses it to another person, the sender can

---

of Ontario v. Quon, 130 S. Ct. 2619, 2630, 2632 (2010) ("Although as a general matter, warrantless searches are per se unreasonable under the Fourth Amendment, there are a few specifically established and well-delineated exceptions to that general rule. . . . [Warrantless searches that are] motivated by a legitimate work-related purpose . . . [and are] not excessive in scope [are reasonable]." (citations and internal quotation marks omitted)); LAFAVE, *supra* note 61, § 2.6(f) ("[A] letter writer's expectation of privacy ordinarily terminates upon delivery of the letter." (citation and internal quotation marks omitted)); *supra* Part IV.B.2 (discussing the validity of third-party doctrine). In sum, the few cases that have dealt with e-mail outside the third-party doctrine and employment law contexts *have* used the reasonable expectation of privacy test to protect citizens' privacy interests in their e-mail.

294. United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable."); *Ex parte* Jackson, 96 U.S. 727, 733 (1887) ("The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household.").

295. Ray, *supra* note 158, at 205 (citing LAFAVE, *supra* note 61, § 2.6).

296. United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996).

297. *Id.* at 418.

298. *Id.* at 417.

reasonably expect the contents to remain private and free from the eyes of the police absent a search warrant founded upon probable cause."[299]

More recently, the Sixth Circuit dealt with a case involving a warrantless search of e-mail in *United States v. Warshak*.[300] The defendants in *Warshak* were convicted of mail fraud, bank fraud, and money laundering.[301] At trial, the evidence against them had been based in large part upon 27,000 e-mails that law enforcement officials obtained from Warshak's Internet service provider ("ISP") without a warrant.[302] In a line of reasoning similar to that found in *Maxwell*,[303] the Sixth Circuit noted the Fourth Amendment protections afforded regular mail by *Ex parte Jackson*[304] and *United States v. Jacobsen*[305] and then stated that

> Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection. . . . Email is the technological scion of tangible mail, and it plays an indispensable part in the Information Age.[306]

Based on this reasoning, the Sixth Circuit held that citizens unequivocally "enjoy[] a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP."[307] As such, the Sixth Circuit used *Katz's* reasonable expectation of privacy test to protect citizens' privacy interests in their e-mail.

---

299. *Id.* (citing Gouled v. United States, 255 U.S. 298 (1921)).

300. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

301. *Id.* at 275.

302. *Id.* at 282.

303. In fact, the *Warshak* court cited *Maxwell* to support the proposition that senders of e-mail expect the contents of their messages to remain private. *See id.* at 284 (citing United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996)).

304. *Ex parte* Jackson, 96 U.S. 727 (1887).

305. United States v. Jacobsen, 466 U.S. 109 (1984).

306. *Warshak*, 631 F.3d at 285–86.

307. *Id.* at 288. The reader should note, however, that the Sixth Circuit ultimately held that the exclusionary rule did not apply in this case because law enforcement officials relied in good faith upon the Stored Communications Act ("SCA") when they obtained Warshak's e-mails from his ISP. *Id.* at 288–92. The court ensured that future good faith defenses would not succeed by holding that "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional." *Id.* at 288.

The *Warshak* court further demonstrated the reasonable expectation of privacy test's ability to protect citizens' Fourth Amendment interests by explaining why third-party doctrine fails to frustrate citizens' reasonable expectation of privacy in their e-mail. Some commentators have pointed to third-party doctrine as a major reason why the reasonable expectation of privacy test will fail to protect citizens from warrantless e-mail searches.[308] *Warshak* shows why these worries lack foundation by differentiating between the distinct acts of conveying a communication to an intermediary and conveying a communication to the general public. Since it is impossible to send an e-mail without it passing through the ISP's servers, "the ISP is the functional equivalent of a post office or a telephone company."[309] Once this reality is acknowledged, it is clear that third-party doctrine does not destroy citizens' reasonable expectation of privacy in their e-mail. "[T]he police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call."[310] Since the ISP and its servers are the e-mail equivalent of a post office or phone company, it stands to reason that the police also may not compel ISPs to turn over a subscriber's e-mail without triggering the Fourth Amendment. This line of reasoning further demonstrates that *Katz's* reasonable expectation of privacy test is capable of protecting citizens' privacy interests in the most important of all modern technologies: the Internet.

V. THE JUDICIARY VS. THE LEGISLATURE: DETERMINING SOCIETY'S EXPECTATIONS

As the preceding sections have demonstrated, ample case law exists from both the Supreme Court and lower federal courts demonstrating *Katz's* continued ability to protect citizens' Fourth Amendment rights in this age of advancing technology. Most importantly, the High Court consistently demonstrates steadfast support of citizens' privacy rights in the most private of all places—the home.[311] Outside the home, there is also significant language in

308. *See, e.g.*, Weaver, *supra* note 6, at 1193–94 (noting that since electronic communications and cloud computing are voluntarily conveyed to third parties (i.e., ISPs), the Court's rulings in cases like *Smith v. Maryland* could indicate that such actions are not protected by the reasonable expectation of privacy test).

309. *Warshak*, 631 F.3d at 286.

310. *Id.*

311. *See supra* Part IV.B.1 (discussing the Court's steadfastness in protecting the privacy of the home).

cases like *Knotts*,[312] *Karo*,[313] *Dow Chemical*,[314] and *Kyllo*[315] to suggest that dragnet-type law enforcement surveillance would not be upheld under the current framework created by *Katz*.[316] And, most recently the Court protected a defendant's Fourth Amendment rights in his public movements in *Jones*.[317] Rulings in lower courts protecting citizens' privacy from warrantless searches in the realm of video surveillance and e-mail further demonstrate the reasonable expectation of privacy test's continued vitality in Fourth Amendment jurisprudence.[318]

None of this is to say, however, that *Katz's* reasonable expectation of privacy test is perfect in every way. The abundant legal scholarship arguing to the contrary makes that clear. Any legal standard based upon the reasonable expectations of society presents courts "with a hard issue."[319] But the important point is that this issue is the "correct" one.[320] Since the primary goal of the Fourth Amendment is to protect citizens from unregulated government intrusion,[321] it only makes sense to look to society's expectations of privacy when determining the bounds of the Amendment.

While other commentators recommend logical replacements for the reasonable expectation of privacy test, these tests either: (1) ask questions that are just as difficult to answer as the reasonable expectation of privacy test;[322] or (2) advocate for bright-line rules at

312. United States v. Knotts, 460 U.S. 276 (1983).

313. United States v. Karo, 468 U.S. 705 (1984).

314. Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

315. Kyllo v. United States, 533 U.S. 27 (2001).

316. *See supra* Part IV.B.3 (discussing public privacy).

317. United States v. Jones, 132 S. Ct. 945 (2012).

318. *See supra* Part IV.C (discussing the reasonable expectation of privacy test in lower courts).

319. LAFAVE, *supra* note 61, § 2.1.

320. *Id.*

321. *See, e.g.*, Illinois v. McArthur, 531 U.S. 326, 330 (2001) ("[T]his Court has interpreted the [Fourth] Amendment as establishing rules and presumptions designed to control conduct of law enforcement officers that may significantly intrude upon privacy interests.").

322. *See, e.g.*, Casey, *supra* note 8, at 1026 ("The reasonable expectation of privacy standard should be abandoned in favor of a test that reclaims the original language of the Fourth Amendment—the right to be secure. Removing the reasonable expectation of privacy from our Fourth Amendment discourse will resolve some of the confusion that has plagued jurisprudence in the post-Katz era."); Henderson, *supra* note 158, at 546 (arguing in favor of "jettisoning the [reasonable expectation of privacy] test in favor of a dictionary definition of search").

the expense of determining what level of privacy society actually expects.[323] The reasonable expectation of privacy test, though not infallible, asks the right question and typically achieves just results. This Note urges commentators to realize that, whatever test is used for determining privacy expectations, it will not always be easy to reach "correct" conclusions. The reasonable expectation of privacy test has performed well to this point, and the Court's recent ruling in *Jones* seems to point toward similarly promising results in the future.

One aspect of the Court's reasonable expectation of privacy jurisprudence, however, does warrant further discussion. As noted above, the Court's application of third-party doctrine in the reasonable expectation of privacy context has spurred significant scholarly debate.[324] And this debate can only be expected to grow as citizens transmit more and more information over the Internet. As Justice Sotomayor pointed out in her *Jones* concurrence:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[325]

Thus, the issue of third-party doctrine, and how it relates to the Fourth Amendment and technology, is almost certainly an issue that the Court will face in future cases. This final Part explores whether courts or legislatures are best suited for determining society's privacy expectations with relation to modern technology. It concludes that there are benefits and drawbacks to each branch of government making such determinations and that it would be unwise to allocate all responsibility for such decisions to just one of them. This Part then goes on to make a modest suggestion. Courts should explicitly recognize that social policy plays a significant role in determining society's privacy expectations. As such, courts should adopt a policy of looking to legislative treatment of novel technologies in determining how those technologies implicate societal expectations of privacy.

---

323. *See, e.g.*, Penney, *supra* note 160, at 506 (arguing that the reasonable expectation of privacy test should be replaced with an "[e]conomically-informed cost-benefit analysis").

324. *See supra* Parts IV.B.2–3.

325. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

Such a policy will help ensure that courts stay in tune with what society deems a reasonable expectation of privacy in this age of ever-advancing technology.

A. Courts or Legislatures?

Courts admittedly have institutional limitations that at times make it difficult for them to accurately assess society's expectations. This is particularly true in the field of technology, since courts often "lack the institutional capacity to easily grasp the privacy implications" of rapidly changing technology.[326] To help overcome this inherent difficulty, a good case can be (and has been) made that courts should take a back seat to legislatures in making decisions about advancing technology.

On a basic level, the determination of society's expectations clearly has a major social policy aspect. As such, at least one lower court has argued that decisions regarding the impact of advancing technology on citizens' privacy rights are policy decisions that ought to be left to the legislature.[327] Professor Kerr has argued that, due to the institutional limitations of courts, judges often have trouble grasping the privacy implications of new technologies because they do not have time to fully learn how those technologies will develop.[328] Due to these circumstances, Professor Kerr believes that "legislative rule-creation offers significantly better prospects for the generation of balanced, nuanced, and effective investigative rules involving new technologies."[329] Legislatures, he argues, have a level of flexibility the courts do not have, which allows them to adapt more readily and amend laws as technology quickly changes—an ability that courts in our legal system simply lack.[330] Kerr also points out that court-made law is almost always ex post, that is, it looks back at situations that have already occurred and fashions a rule for that past occurrence.[331] Such law, Kerr urges, causes the common law to lag behind legislation in the context of rapidly advancing technology, which typically looks to the present and future.[332]

---

326. Kerr, *supra* note 6, at 858.

327. United States v. McNulty, 47 F.3d 100, 106 (4th Cir. 1995) ("As new technologies continue to appear in the marketplace and outpace existing surveillance law, the primary job of evaluating their impact on privacy rights and of updating the law must remain with the branch of government designed to make such policy choices, the legislature.").

328. Kerr, *supra* note 6, at 858–59.

329. *Id.* at 859.

330. *Id.* at 871.

331. *Id.* at 868.

332. *Id.*

Though Professor Kerr makes several good points, many commentators are hesitant to abandon the common law in an area of law that is becoming increasingly important to citizens' everyday lives and has such significant constitutional implications.[333] Also, the legislature's ability to handle technological issues is perhaps not quite as straightforward as Professor Kerr argues. While Congress can often respond more quickly to technological advances than courts, it is unlikely to frequently revisit issues once it has passed legislation on them.[334] Put simply, legislatures tend to have a short attention span.[335] As such, legislative decisions are just as prone to becoming outdated by the rapid advance of technology as judicial opinions are. In some circumstances this may create even greater confusion than what might result from outdated common law. While the judicial community is constantly evaluating and reevaluating the common law, congressionally enacted statutes may remain untouched for long periods of time. In the context of rapidly advancing technology, such statutes could actually become "straitjackets" that hamper the growth and development of the technology they seek to regulate. [336]

---

333. *See, e.g.*, Blitz, *supra* note 157, at 1467 (arguing that, although legislatures have considered laws setting special warrant requirements for high-tech surveillance, "courts should insist on similar requirements as a constitutional matter. Even when a state or locality is unwilling to protect the character of its public space, this does not mean that individuals within that state or locality should therefore be without safeguards against intrusive video monitoring that undercuts core Fourth Amendment interests"); Swire, *supra* note 167, at 905 (criticizing Professor Kerr's argument that "Congress can do a better job than the courts at creating the law for high-tech surveillance" and arguing that "Fourth Amendment [jurisprudence] should continue to play a role in governing electronic surveillance and other high-tech searches. At a minimum, the Court should announce basic principles for how surveillance can be conducted, with Congress then supplying the details").

334. *See, e.g.*, Suzanna Sherry, *Haste Makes Waste: Congress and the Common Law in Cyberspace*, 55 VAND. L. REV. 309, 312 (2002) ("[L]egislation designed to address questions raised by rapidly changing technology is likely to become obsolete equally [as] quickly [as court decisions] . . . . [O]nce Congress has enacted legislation regulating a particular subject, it is unlikely to revisit the issue for some time.").

335. *See, e.g.*, *Advocacy Over and For the Long Term*, CMT'Y TOOL BOX, http://ctb.ku.edu/en/tablecontents/sub_section_main_1267.aspx (last visited Oct. 4, 2012) ("Unfortunately, as short as the attention span of the public sometimes is, that of legislators and other policy makers is often even shorter—for many, no longer than the time between elections.").

336. Sherry, *supra* note 334, at 312. An apt example of Congress being too hasty in passing laws regulating a modern technology is its reaction to the rise of the railroad. At the beginning of the twentieth century, Congress passed a series of laws intended to regulate railroad shipping

There is also something to be said against rejecting the common law system upon which our legal system is based. The beauty of the common law system is its recognition that the best legal rules are achieved by pitting two zealous advocates against one another, allowing them to delve into and explain the redeeming qualities of each side of the problem, and then allowing a neutral arbiter to decide which among those arguments is best. By replicating this process hundreds and hundreds of times for virtually every possible legal topic, our legal system creates a pseudo-democracy for arriving at optimal legal solutions.[337] This process would be lost in the technology arena by giving the legislature sole decision-making authority over technological privacy issues.

Many of the privacy issues presented by advancing technology would be largely uncontroversial at the congressional level. For instance, who doesn't want the privacy of his e-mail to be protected? But such unopposed legislation is dangerous. Without a strong voice for the opposing side, the potential for poorly drafted laws greatly increases, and with enough such "easy" decisions to make, there is also the potential that Congress will put off making more difficult and controversial choices.[338] As another commentator argues, putting decisions about the privacy implications of technology solely in the hands of the legislature could result in a *reduction* of citizens' rights.[339] Historically, law enforcement authorities, when left unchecked by the courts, have been able to influence Congress to pass laws requiring *less* regulation of law enforcement tactics.[340] Multiple

---

rates and thus prevent monopolies. These laws remained unchanged until 1970. In the interim, the automobile and airplane rose to prominence, thus eliminating the possibility of a railroad monopoly on interstate shipping and travel. Rather than serving to prevent a monopoly, the rate-regulating laws ended up leading to the bankruptcy of many railroads. *Id.* at 312–13.

337. Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1745 (1995) ("What is special about the common law . . . is its constructive function. What recommends it is the process that it offers, with its partial answers, to repeated if slightly varied questions, in a range of contexts with a world of different talent and ideals. If, as Levi said, the common law is democratic, it is democratic not because many people get to vote together on what the law should mean, but because many people get to say what the common law should mean, each after the other, in a temporally spaced dialogue of cases and jurisdictions. Unlike other lawmaking, what defines the process of the common law is small change, upon which much large change gets built; small understandings with which new understandings get made.").

338. *See* Sherry, *supra* note 334, at 314–15.

339. Swire, *supra* note 167, at 914–16.

340. *See id.* at 914–15 (offering the events of September 11, 2001 and the USA PATRIOT Act as an example of this proposition).

commentators have also pointed out the inarguable fact that Congress often looks to the rulings of the Supreme Court and other lower courts in coming to decisions about legislation.[341] Putting the determination of technological privacy interests solely in the hands of legislatures would deprive those bodies of this benefit.

With the foregoing arguments in mind, it appears there is no clear-cut answer to the question of which branch, the legislative or judicial, is best suited to deal with advancing technology. While the judiciary may be somewhat slower in responding to technological advancement due to the backward-looking nature of deciding cases, the common law system allows it to constantly reevaluate past decisions. The legislature, on the other hand, offers the potential to respond to technological advancements rapidly by quickly passing legislation. But such speed is at times, as one commentator coyly put it, "expended careening around blind corners."[342] Legislatures have short attention spans. Sometimes they act quickly, but then fail to touch on an issue again for a long time, which may ultimately result in more harm than good. As such, it does not appear wise to alter the status quo in the technological privacy arena. Each branch should continue to deal with such questions as they arise. This will ensure that an adequate system of checks and balances continues to exist between these two branches.[343]

B. Legislative Insight into Society's Reasonable Expectations

This does not mean, however, that intra-branch improvements cannot be made. Courts do, at times, fail to correctly assess societal expectations.[344] To remedy this, it would be useful for courts to

341. *See, e.g.*, *id.* at 915–16 ("Supreme Court decisions have played a primary role in prompting and shaping privacy legislation to date. Congressional actions, when they have occurred, have generally given far less protection than the Fourth Amendment norm of probable cause warrant issued by a neutral magistrate."); Lessig, *supra* note 337, at 1753 ("Constitutional law is fundamentally concerned with who should decide what constitutional questions when. My suggestion here is that we rely for the moment on lower court judges, to give the law the material with which to understand this new realm.").

342. Sherry, *supra* note 334, at 317.

343. *See, e.g.*, Swire, *supra* note 167, at 913–14 (arguing that "courts and Congress working together can likely produce better results than Congress alone"); *see also infra* note 368 for an example of this system at work.

344. *See, e.g.*, United States v. Miller, 425 U.S. 435 (1976). In this case, the Court, applying third-party doctrine, held that citizens do not have a reasonable expectation of privacy in their bank records because checks, deposit slips, and financial records

> are not confidential communications but negotiable instruments to be used in commercial transactions. [They] . . . contain only

explicitly recognize that the determination of society's reasonable expectations has a distinct social policy component. With this fact in mind, courts should adopt a policy of looking to the way legislatures have dealt with novel technologies in determining how those technologies implicate societal expectations of privacy.[345] Such a policy would recognize the legislature's role in determining social policy. By including such analysis in Fourth Amendment and technology jurisprudence, courts can look to legislatures for valuable insight into societal expectations while the many benefits of the common law system are still retained. In addition, maintaining a strong presence by both branches in the realm of Fourth Amendment technology law will ensure continued discourse between the legislature

> information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.

Id. at 442. This ruling misconstrued societal expectations. Does society really think it unreasonable for citizens to believe that their bank records are entitled to at least *some* privacy?

Congress ultimately remedied this situation, passing the Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641, which prohibited government officials from accessing or obtaining "copies of, or the information contained in[,] the financial records of any customer from a financial institution unless [one of several exceptions applies]." Right to Financial Privacy Act of 1978 § 1102, 12 U.S.C. § 3402 (2006). This situation demonstrates why having both the judiciary and legislature making privacy decisions is the optimal situation. If one missteps, the other can step in with curative measures.

345. The D.C. Circuit utilized reasoning comparable to this suggestion in its ruling in *Jones*. *See* United States v. Maynard, 615 F.3d 544, 563–65 (D.C. Cir. 2010), *aff'd on other grounds sub nom.* United States v. Jones, 132 S. Ct. 945 (2012). Though the D.C. Circuit's result was affirmed on other grounds by the Supreme Court, its reasoning still demonstrates how this Note's recommendation would work. In determining whether Jones had a reasonable expectation to be free from GPS surveillance for thirty days, the D.C. Circuit found significant that the California legislature had "specifically declared [that] 'electronic tracking of a person's location without that person's knowledge violates that person's reasonable expectation of privacy,' and implicitly but necessarily thereby required a warrant for police use of a GPS." *Maynard*, 615 F.3d at 564 (citing CAL. PENAL CODE § 637.7 (West 2010)). It also noted that several other states have enacted similar statutes. *See id.* (citing UTAH CODE ANN. §§ 77-23a-4, 77-23a-7, 77-23a-15.5 (LexisNexis 2008); MINN. STAT. ANN. §§ 626A.37, 626A.35 (2009); FLA. STAT. ANN. §§ 934.06, 934.42 (West 2006); S.C. CODE ANN. § 17-30-140 (Supp. 2011); OKLA. STAT. ANN. tit. 13, §§ 176.6, 177.6 (2011); HAW. REV. STAT. §§ 803-42, 803-44.7 (1993); 18 PA. CONS. STAT. ANN. § 5761 (West 2000)). The D.C. Circuit concluded that "these state laws are indicative that prolonged GPS monitoring defeats *an expectation of privacy that our society recognizes as reasonable*." *Id.* (emphasis added). Thus, using a line of reasoning virtually identical to the one this Note espouses, the D.C. Circuit looked to how legislatures had handled the question of GPS surveillance in determining whether Jones had a reasonable expectation of privacy.

and judiciary and maintain a healthy system of checks and balances. Such discourse, in the long run, should lead to optimal results.

The realm of e-mail provides an example of how this policy would achieve desirable results. As noted above, the Court has yet to deal with a Fourth Amendment case that implicates the Fourth Amendment and e-mail.[346] The recent decision by the Sixth Circuit in *Warshak* [347] provides a promising example of how the reasonable expectation of privacy test can be applied in a manner that protects citizens' e-mail privacy. But this is not the only place the Court would be able to look if it had to rule on a Fourth Amendment e-mail case tomorrow. Congress, in its capacity as representative of the people, has legislated heavily on privacy and electronic communication. Under this Note's proposed policy, the Court would also look to how Congress has handled e-mail in determining what society's privacy expectations in e-mail are.

In 1986, Congress passed the Electronic Communications Privacy Act,[348] which amended federal wiretap law to include electronic communications. The aim of the Act is to "protect privacy interests in personal and proprietary information . . . [and prevent] the unauthorized interception of electronic communications."[349] The Act explicitly includes e-mail in its definition of "electronic communications"[350] and requires law enforcement officers to apply to a federal judge for permission to intercept e-mail communications.[351] The Senate Report noted that, at the time, legal protections for electronic mail were "weak, ambiguous, or non-existent, and that electronic mail [was] legally as well as technically vulnerable to unauthorized surveillance."[352] The Senate passed the Act to remedy this situation and "to ensure the continued vitality of the fourth amendment."[353] The Senate Report also noted that "[p]rivacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens."[354]

346. *See supra* Part IV.C.2.

347. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

348. Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2522 (2006)).

349. S. Rep. No. 99-541, at 1, 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555.

350. *Id.* at 8 (including a definition of "electronic mail" in the report's glossary of terms that count as communications).

351. 18 U.S.C. § 2516 (2006).

352. S. Rep. No. 99-541, at 4.

353. *Id.* at 5.

354. *Id.*

If the Supreme Court were to adopt the policy this Note suggests and make a point of looking at how legislatures have handled technologies that are novel[355] to the Court, the Electronic Communications Privacy Act and accompanying Senate Report would make its decision in a Fourth Amendment case involving e-mail relatively straightforward. Let us assume a case with the following fact pattern: Charles is suspected of conducting illegal gambling activities online. Law enforcement officials, without obtaining a warrant, intercept several of Charles's e-mails, which lead to his arrest and conviction for illegal gambling. Charles appeals, alleging that the e-mail evidence should have been suppressed as "fruit of the poisonous tree."[356] Charles loses his appeal below and the Supreme Court grants certiorari.

When Charles's case comes before the Supreme Court, the Court's decision would hinge on whether Charles had a reasonable expectation of privacy in his e-mail communications. Some of the Justices might look to third-party doctrine to determine the outcome of Charles's case. Under this reasoning, Charles's chances of winning may be slim, since almost all e-mails pass through a third-party ISP before reaching the intended recipient.[357] Thus, since Charles conveyed his e-mail messages to a third party, some Justices might argue he no longer had a reasonable expectation of privacy in them under long-standing Supreme Court precedent.[358] But is this really true? As Justice Sotomayor noted in *Jones*,

> I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year . . . [even though] [p]eople disclose the . . . URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers.[359]

Justice Sotomayor's observation seems to make a lot of sense. Just because all information passed over the Internet goes through an ISP

355. In this context, "novel" is intended to mean a technology the Court is hearing a case about for the first time.

356. Nardone v. United States, 308 U.S. 338, 341 (1939).

357. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).

358. *See, e.g.*, Smith v. Maryland, 442 U.S. 734, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." (citing multiple Supreme Court opinions, including United States v. White, 401 U.S. 745 (1971) (plurality opinion))).

359. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

should not mean it loses all Fourth Amendment protection[360]—millions of people disclose very personal information over the Internet every day, sometimes even while performing the simplest of tasks.[361] Holding that third-party doctrine deprives *all* of this information of a reasonable expectation of privacy is simply an approach that "is ill-suited to the digital age."[362]

If the Court were to have, as this Note advocates, a policy in place for looking to how the legislature has dealt with e-mail technology, it would see that a strict application of third-party doctrine to e-mail is inconsistent with society's privacy expectations. The Electronic Communication Privacy Act and the Senate Report accompanying it make abundantly clear that citizens *do* expect a certain degree of privacy in their e-mail.[363] Indeed, one of the primary aims of the Electronic Communications Privacy Act was to protect citizens' "privacy interests."[364] If such an expectation has been statutorily recognized by Congress—the representative of the people—the Court cannot possibly hold that citizens do not have a reasonable expectation of privacy in e-mail. As one commentator pointed out, "[t]he people's voice in the governmental context is the legislature and when the legislature expressly recognizes an expectation of privacy, a court should not find that expectation socially unreasonable."[365] Thus, society *is* prepared to recognize as reasonable Charles's expectation of privacy in his e-mail and the Court should rule in his favor. This ruling would also be consistent with *Warshak*,[366] the only federal circuit court opinion that has thus far addressed e-mail in the Fourth Amendment context.[367]

By looking to legislative reaction to novel technology, courts will be able to more accurately gauge societal expectations, which will lead to a Fourth Amendment jurisprudence that continues to protect

360. *See id.* ("I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.").

361. *Id.* ("[In the digital age,] people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.").

362. *Id.*

363. *See, e.g.*, Ray, *supra* note 158, at 225-27 (arguing that when Congress passed the Electronic Communications Privacy Act of 1986, "it explicitly recognized the public's expectation of privacy in electronic communications").

364. S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555.

365. Ray, *supra* note 158, at 226 (internal citation omitted).

366. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

367. *See supra* Part IV.C.2 (addressing how lower courts have applied the reasonable expectation of privacy test in the context of e-mail).

citizens' privacy interests. This is not to say that courts should always rule based on what a legislature has done. But at least in the context of society's expectations as they relate to new technologies, legislatures can often provide courts with a window into the psyche of society and thus what society truly deems to be "reasonable."

CONCLUSION

Samuel Warren and Louis Brandeis once observed that "[t]he intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual."[368] This observation is even truer now than it was then. The rapid advance of technology in today's society has made it increasingly easy for the government to peer into citizens' private lives. In some ways this is a good thing—it makes for more efficient and effective law enforcement. But as Warren and Brandeis pointed out, citizens do not always want to be in the public eye—they need at least some privacy. The Supreme Court understands this and protects citizens' privacy interests by holding unconstitutional any warrantless search that violates a reasonable expectation of privacy.[369]

As this Note has demonstrated, the reasonable expectation of privacy test has been able to protect citizens' privacy interests, even in the face of modern technology. Most importantly, the Supreme Court's Fourth Amendment jurisprudence has been steadfast in its protection of privacy in the home.[370] Additionally, language in several of its Fourth Amendment and technology opinions indicates that citizens also have a reasonable expectation of privacy in public.[371] The Court's recent ruling in *Jones* and the concurring opinions accompanying it bode well for continued protection of citizens' public privacy rights.[372] Further, in areas such as video surveillance and e-mail searches—Fourth Amendment issues that the Court has yet to rule on—lower courts seem to be applying the reasonable expectation

368. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

369. *See supra* Part II (discussing the background of *Katz* and the establishment of the reasonable expectation of privacy test).

370. *See supra* Part IV.B.1 (discussing the Court's protection of privacy in the home).

371. *See supra* Part IV.B.3 (discussing how the Court's Fourth Amendment jurisprudence indicates that citizens have a reasonable expectation of privacy in some public places).

372. *See supra* Part IV.B.4 (analyzing the majority and concurring opinions in *Jones*).

of privacy test in a manner that protects citizen privacy.[373] Such results further indicate that the Court's current Fourth Amendment jurisprudence is up to the task of protecting privacy interests from the specter of advancing technology.

But this is not to say that the reasonable expectation of privacy test is perfect in every way. As noted above, determining what society reasonably expects is not an easy task.[374] But when the privacy expectations of this nation's citizens are on the line, it is the right question to be asking. As courts move forward in this age of advancing technology, they should be cognizant of the policy determinations involved in gauging societal expectations. Since social policy is often best determined by legislatures, it makes sense for courts to look to how legislative bodies have dealt with novel technologies when determining society's expectations of privacy. Such a policy will help courts accurately reflect societal expectations and ensure that the will of the people, as expressed by the legislature, is sufficiently protected by future Fourth Amendment jurisprudence.[375]

Katz is not dead yet, nor will its grave be dug anytime soon, so long as courts stay in tune with societal expectations and continue to apply the reasonable expectation of privacy test in a manner that protects citizens' reasonable privacy interests from encroachment by law enforcement's use of advancing technology.

Daniel T. Pesciotta[†]

373. *See supra* Parts IV.C.1–2 (discussing lower courts' application of the reasonable expectation of privacy test).

374. *See* LAFAVE, *supra* note 61, § 2.1 (describing the reasonable expectation of privacy test as presenting courts "with a hard issue"); *supra* note 324 and accompanying text.

375. *See supra* Part V.B (arguing that courts passing Fourth Amendment judgment on novel technologies should look to legislatures for guidance on how to determine what society deems a reasonable expectation of privacy).

† © 2012. J.D. Candidate, 2013, Case Western Reserve University School of Law, Cleveland, Ohio. I would like to thank Dean Jonathan Entin for his many thoughtful and insightful suggestions. I would also like to thank Robert Cheren, Emily Cohen, and Isaac Figueras for reading earlier drafts of this Note and Linda Thompson for her continued support throughout the Note writing process.

SCHOOL OF LAW

CASE WESTERN RESERVE
UNIVERSITY