THE FOURTH AMENDMENT AND NEW TECHNOLOGIES: THE MISAPPLICATION OF ANALOGICAL REASONING

Marc McAllister*

I. INTRODUCTION

The Fourth Amendment prohibits "unreasonable searches and seizures."[1] While the Fourth Amendment prevents many forms of warrantless police investigation, methods of investigation not amounting to a "search"[2] or "seizure"[3] are exempt from Fourth Amendment protection.[4]

To determine whether a particular form of investigation constitutes a "search," courts generally employ the *Katz* test.[5] Under the *Katz* test, a

---

* Associate Professor, Florida Coastal School of Law; J.D., University of Notre Dame Law School. The author would like to thank Dr. Raoul A. Arreola for his invaluable assistance in designing the survey outlined below, along with students Alexandra Whitehead and Katherine Garro for their help in administering the survey. The author would also like to thank Professors Benjamin Priester and Joanmarie Davoli for their helpful feedback on this article.

1. U.S. CONST. amend. IV.
2. The term "search" is a legal term of art, and is not always consistent with its ordinary dictionary definition. *See* Kyllo v. United States, 533 U.S. 27, 32 n.1 (2001) (contrasting the Fourth Amendment definition of "search" with the dictionary definition of "search"). Indeed, many routine forms of police surveillance are not considered a Fourth Amendment "search," such as a dog sniff at an airport, even where the obvious purpose of the activity is to uncover evidence of a crime. *See* United States v. Place, 462 U.S. 696 (1983).
3. Fourth Amendment claims often involve seizures of persons and seizures of property. Under Fourth Amendment precedent, a "seizure" of property occurs "when there is a meaningful interference with an individual's possessory interest in property." United States v. Jacobsen, 466 U.S. 109, 113 (1984). Seizures of persons include both (1) investigative detentions of limited scope and duration which must be supported by a reasonable suspicion of criminal activity; and (2) arrests, which are reasonable only if supported by probable cause. United States v. Davis, 94 F.3d 1465, 1467-68 (10th Cir. 1996).
4. To determine whether a particular form of surveillance complies with the Fourth Amendment, courts typically follow a three-step approach. In the first step, courts consider whether a Fourth Amendment "search" or "seizure" has occurred. If a "search" or "seizure" has occurred, courts then determine whether the particular investigatory action was "reasonable," which generally requires a previously secured warrant. *See* Katz v. United States, 389 U.S. 347, 357 (1967) ("searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment"). If a court concludes that an unreasonable search or seizure has indeed occurred, the court finally determines the appropriate remedy, usually evidence exclusion. *See* Mapp v. Ohio, 367 U.S. 643, 655 (1961) (establishing the general rule that "all evidence obtained by searches and seizures in violation of the Constitution is . . . inadmissible in a state court").
5. *See* Smith v. Maryland, 442 U.S. 735, 739-40 (1979) ("In determining whether a particular form of government-initiated electronic surveillance is a "search" within the meaning of the Fourth Amendment, our lodestar is *Katz*."). As the Court recently clarified, the *Katz* test governs all

"search" occurs only when "the government['s] [conduct] violates a subjective expectation of privacy that society recognizes as reasonable."[6] Under this test, if society would not recognize an asserted expectation of privacy as reasonable, no "search" has occurred,[7] and warrants are not required.[8]

During the forty-five years in which *Katz* has governed, courts have exempted many forms of police surveillance from Fourth Amendment protection. The Supreme Court's early "search" cases involved police use of undercover informants,[9] garbage can searches,[10] dog sniffs,[11] aerial surveillance of private property,[12] and pen registers,[13] all of which resulted in no "search," hence no constitutional protection.

"search" questions that do not involve an actual physical trespass. *See* United States v. Jones, 132 S.Ct. 945, 950 (2012) ("the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test) (emphasis in original).

6. *Kyllo*, 533 U.S. at 33. *See also Katz*, 389 U.S. at 360 (Harlan, J., concurring) ("there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").
7. *See Smith*, 442 U.S. at 739-40 ("Consistently with *Katz*, this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action.").
8. In the traditional view of the Fourth Amendment, police must generally obtain a warrant before they may search or seize, and failure to do so renders the search "*per se* unreasonable." *See Katz*, 389 U.S. at 357 ("'Over and again this Court has emphasized that . . . searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment"); Johnson v. United States, 333 U.S. 10, 13-14 (1948) ("The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime."). *See also* Tracey Maclin, *When the Cure for the Fourth Amendment is Worse than the Disease*, 68 S. CAL. L. REV. 1 (1994) (arguing that that the purpose of the Fourth Amendment is to control executive power, and that it does so via a strong preference for searches and seizures conducted pursuant to warrants).
9. *See* United States v. White, 401 U.S. 745 (1971) (ruling that a person does not have a justifiable and constitutionally protected expectation that a person with whom he is conversing will not reveal the conversation to the police because, by speaking, a person knowingly exposes his thoughts to another).
10. *See* California v. Greenwood, 486 U.S. 35 (1988) (ruling that a person does not have a reasonable expectation of privacy in garbage left outside the curtilage of a home for trash removal because "garbage bags left on or at the side of a public street are readily accessible to . . . other members of the public," including the police).
11. The Supreme Court has ruled on two occasions that dog sniffs do not constitute Fourth Amendment "searches," once in the airport involving a passenger's luggage, United States v. Place, 462 U.S. 696 (1983), and once on a public road where a dog was employed to sniff around a car, Illinois v. Caballes, 543 U.S. 405 (2005).
12. *See, e.g.*, California v. Ciraolo, 476 U.S. 207 (1986) (finding no reasonable expectation of privacy in visual observations by officers flying over defendant's property from 1000 feet above, in navigable airspace, even though the defendant had erected a 10-foot high fence around the yard which would have prevented the same ground-level observations); Florida v. Riley, 488 U.S. 445 (1989) (upholding as not a "search" police observation of the interior of a partially covered

Recent Fourth Amendment "search" cases implicate more sophisticated surveillance methods, including public camera monitoring[14] and devices capable of "seeing through" walls or clothing.[15] Even in cases involving sophisticated technologies, courts have often permitted law enforcement to dispense with the usual requirements of a warrant and probable cause by rejecting the defendant's claimed expectation of privacy.[16]

In rejecting Fourth Amendment claims involving warrantless use of sophisticated technologies, courts often rely upon analogies to prior "search" cases, but these supposed analogies are so far removed from the new forms of surveillance that analogies to them only confuse, rather than clarify, the actual analysis required by *Katz*. The *Katz* test contemplates whether "society would reasonably expect privacy"[17] in the particular case at hand, expectations that are fluid and case-specific.[18] Given the case-

---

greenhouse in Riley's backyard while circling 400 feet above the greenhouse in a police helicopter); Dow Chem. Co. v. United States, 476 U.S. 227 (1986) (upholding as not a "search" EPA's photographing of Dow Chemical's 2000-acre outdoor industrial complex from altitudes of 12,000, 3,000, and 1,200 feet with a "standard, floor-mounted, precision aerial mapping camera").

13. Smith v. Maryland, 442 U.S. 735 (1979) (upholding as not a "search" the warrantless police use of a pen register, installed by the telephone company upon police request, through which police were able to obtain the numbers dialed from defendant's home telephone).
14. *See* United States v. Jones, 132 S.Ct. 945, 963 (2012) (Alito, J., concurring).
15. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding that warrantless police use of a thermal imaging device to scan the defendant's home violated his reasonable expectation of privacy because device was not in "general public use" and because it enabled police to "explore details of the home that would previously have been unknowable without physical intrusion"). *See also* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 8 (University of Chicago Press 2007) (describing more recent handheld devices that produce silhouettes of objects concealed by clothing or cars, some that even reveal anatomical details).
16. *See, e.g.*, United States v. Vela, 486 F.Supp.2d 587 (W.D. Tex. 2005) (upholding as not a "search" the warrantless police use of night vision goggles because such equipment is "commonly used by the military, police and border patrol" and is "available to the public via internet"); Baldi v. Amadon, No. Civ. 02-313-M, 2004 WL 725618 (D.N.H. 2004) (in a civil case, rejecting the defendant's Fourth Amendment argument that a New Jersey conservation officer's use of a night scope to view Baldi's home constituted a Fourth Amendment search); People v. Katz, No. 224477, 2001 WL 1012114, at *2 n.4 (Mich. App. 2001) (per curiam) (finding no Fourth Amendment search for officer's use of night vision equipment).
17. *See* Katz v. United States, 389 U.S. 347, 361 (1957) (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.').
18. In the Fourth Amendment context, the Supreme Court has consistently voiced a preference for a case-by-case approach, a principle that should be more faithfully applied to *Katz* issues involving emerging technologies. As early as 1931, the Court declared, "There is no formula for the determination of reasonableness. Each case is to be decided on its own facts and circumstances." Go-Bart Co. v. United States, 282 U.S. 344 (1931). The Court in *Sibron v. New York* similarly declared, "[t]he constitutional validity of a warrantless search is pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case." 392 U.S. 40, 59 (1968). More recently, Justice Breyer stressed the case-specific nature of Fourth Amendment analysis when he wrote, "I stress the totality of circumstances, however, because were the

specific nature of the *Katz* inquiry, this article contends that analogical reasoning to cases of an earlier technological era is a flawed approach for resolving Fourth Amendment claims;[19] that society's actual expectations of privacy should be examined in a *Katz* analysis; and that the empirical method is the best measure of those expectations.

Two current issues illustrate the flaws of analogical reasoning in a *Katz*-based analysis: the warrantless monitoring of a vehicle's movements by a Global Positioning System device (GPS), and the warrantless police access of certain electronic files and records.

In the GPS tracking cases decided prior to *United States v. Jones*,[20] courts generally permitted police to track vehicles by GPS for lengthy periods of time without warrants and without probable cause,[21] and usually justified that result by analogies to investigative activities far removed from the particular form of surveillance at hand, such as trailing a car by vehicle.[22] Yet, as the five concurring Justices in *Jones* recognized,[23] an

---

circumstances to change significantly, so should the result." Georgia v. Randolph, 547 U.S. 103, 127 (2006) (Breyer, J., concurring). And, just this year, the concurring Justices in *United States v. Jones* noted a variety of factors that would determine expectations of privacy in any particular GPS-tracking case, and concluded that "[t]he best we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking *in a particular case* involved a degree of intrusion that a reasonable person would not have anticipated." 132 S.Ct. 945, 962-63 (2012) (Alito, J., concurring) (emphasis added). *See also United States v. Garcia*, 474 F.3d 994, 997 (7th Cir. 2007) ("the Supreme Court has insisted . . . that the meaning of a Fourth Amendment search must change to keep pace with the march of science").

19. Commentators have begun making similar arguments. *See, e.g.*, Joshua A. Engel, *Doctrinal Collapse: Smart Phones Cause Courts to Reconsider Fourth Amendment Searches of Electronic Devices*, 41 U. MEM. L. REV. 233, 236 (2010) (noting a "growing recognition by courts to treat the difference or similarity between cell phones and containers as one of kind" rather than one of degree, and arguing that this approach should extend to other emerging technologies); Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 U.C.L.A. L. REV. 27 (2008); Bryan Andrew Stillwagon, *Bringing an End to Warrantless Cell Phone Searches*, 42 GA. L. REV. 1165 (2008).

20. 132 S.Ct. 945 (2012).

21. *See, e.g.*, United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010) ("when police have reasonable suspicion that a particular vehicle is transporting drugs, a warrant is not required" to track the vehicle by GPS for a "reasonable period of time"); United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010) (upholding GPS tracking of an individual's movements in his vehicle over a prolonged period as not a search); United States v. Garcia, 474 F.3d 994, 997-98 (7th Cir. 2007) (holding that the use of a GPS tracking device to monitor a vehicle's movements over a prolonged period is not a Fourth Amendment search); United States v. Moran, 349 F. Supp.2d 425, 467 (N.D.N.Y. 2005) (holding that the use of a GPS tracking device to monitor a vehicle's movements is not a Fourth Amendment search where the GPS unit tracked the defendant's vehicle for two days). *But see* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) (holding that the use of a GPS tracking device to monitor an individual's movements in his vehicle over a four-week period is a search).

22. *See Garcia*, 474 F.3d at 997-98 (holding that the use of a GPS tracking device to monitor a vehicle's movements over a prolonged period is not a Fourth Amendment search because GPS tracking is a mere "substitute . . . for an activity, namely following a car on a public street, that is unequivocally *not* a search"); *Marquez*, 605 F.3d 604 (rejecting the defendant's Fourth Amendment challenge to GPS tracking on the grounds that "[a] person traveling via automobile

officer trailing a car turn-by-turn is far less invasive than the long-term monitoring of a vehicle by GPS, and the situations entail very different expectations of privacy.[24]

The same flaw appears in the lower courts' application of the Supreme Court's distinction between the content of various communications, which are protected by the Fourth Amendment, and the addressing information associated with those communications, which are not.[25] While this distinction arose in the Court's early *Katz* cases, most notably *Smith v. Maryland*,[26] this distinction has been erroneously extended to a range of distinct forms of communication.[27]

United States v. Forrester[28] is illustrative. In that case, the Ninth Circuit Court of Appeals analogized the case to *Smith v. Maryland*, which found no expectation of privacy in numbers dialed from a home

---

on public streets has no reasonable expectation of privacy in his movements from one locale to another"); *Moreno*, 591 F.3d at 1216 (upholding GPS tracking of vehicle's movements over a prolonged period as not a search, reasoning that "[t]he only information the [police] obtain[] from [GPS] tracking [of a vehicle] [i]s a log of the locations where [the suspect's] car traveled, information the agents could have obtained by following the car. . . . [which is] unequivocally not a search within the meaning of the Fourth Amendment").

23. Justice Alito's opinion was endorsed by Justices Ginsburg, Breyer, and Kagan. Justice Sotomayor endorsed much of Justice Alito's *Katz*-based reasoning, bringing the total number of Justices who employed a *Katz*-based analysis to five.

24. *See* United States v. Jones, 132 S.Ct. 945, 963 (2012) (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. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."). *See also id.* at 954 (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.'") (emphasis added).

25. *See Smith*, 442 U.S. at 743 ("Although petitioner's conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.").

26. *See id.* at 741-43 (discussing the distinction between the content of communications and the addressing information associated with those communications).

27. *See* United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (collecting cases from the Fourth, Sixth, and Ninth Circuits and district courts in West Virginia, Massachusetts, Connecticut, Maryland, New York, and Kansas, and concluding that "[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation"); *see also* United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (applying the *Smith* assumption of risk doctrine to internet subscriber information, and concluding that there is no legitimate expectation of privacy in such information); United States v. D'Andrea, 497 F.Supp.2d 117, 120 (D.Mass. 2007) ("The *Smith* line of cases has led federal courts to uniformly conclude that internet users have no reasonable expectation of privacy in their subscriber information, the length of their stored files, and other noncontent data to which service providers must have access."). Numerous courts have extended the *Smith* assumption of risk doctrine beyond internet provider information to, *inter alia*, credit card statements, electric utility records, motel registration records, and employment records. *See* United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. April 21, 2008) (collecting cases).

28. 512 F.3d 500 (9th Cir. 2007).

telephone,[29] and reasoned that individuals similarly cannot expect privacy in the websites they visit and the e-mail addresses with which they correspond[30] because that information, like the information in *Smith*, has been knowingly conveyed to a third-party provider.[31] Extending the analogy to *Smith*, the *Forrester* court reasoned that both the pen register and the internet/e-mail address search are minimally intrusive because neither technology acquires the contents of the communication at issue; rather, each technology reveals only the addressing information associated with the particular communication, where expectations of privacy are arguably diminished.[32]

The analogy between phone numbers dialed from a home phone, a specific type of addressing information, and e-mail addresses, another type of addressing information, is plausible on its face. However, *Smith* was decided years before e-mail and internet existed, and the analogy is flawed if it does not comport with the actual expectations of today's society, expectations that are shaped by factors not present in the pre-digital era.

In her concurrence in *Jones*,[33] Justice Sotomayor highlighted this flaw in the *Forrester* rationale. According to Justice Sotomayor, "[t]h[e] [assumption of risk] approach is ill suited to the digital age, in which people

---

29. *See Smith*, 442 U.S. at 743 ("Telephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes . . . . [I]t is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret").

30. *See Forrester*, 512 F.3d at 510 ("We conclude that the surveillance techniques the government employed here are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*.").

31. *See id.* ("*Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment. Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.").

32. *See id.* ("the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here"). *See also id*. ("[E]-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers. When the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed.") *Cf.* Doe v. Prosecutor, Marion Cty., Ind., 566 F.Supp.2d 862, 880 n.6 (S.D. Ind. 2008) (distinguishing between monitoring website IP addresses, which arguably do not "reveal content," and monitoring the URL's of the pages visited, which reveal significantly more content by identifying the particular document with a website that a person views; further noting that a surveillance technique that captures IP addresses would show only that a person visited the New York Times' website at http://nytimes.com, whereas a technique that captures URL's would also divulge the particular articles the person viewed).

33. 132 S.Ct. 945 (2012) (Sotomayor, J., concurring).

reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[34] Given this reality, Justice Sotomayor doubted whether *today's society* would accept the warrantless disclosure of a list of every Web site they had visited, the e-mail addresses with which they have corresponded, and the phone numbers they have dialed,[35] the very issues resolved in the Government's favor in *Forrester* and *Smith*.

Justice Sotomayor's observations become even more significant when applied to cases involving electronic monitoring of a suspect's movements in the absence of a physical trespass, an issue not decided in *Jones*.[36] The assumption of risk rationale, for example, is potentially dispositive in cases where the Government obtains cell site location information directly from a cell phone provider.[37] Given the restrictions *Jones* places upon GPS tracking accomplished by actual trespass, ones that have already prompted changes in methods of investigation,[38] this particular method of surveillance is becoming more popular.[39] With *Smith*'s rationale at the forefront of these unresolved aspects of suspect monitoring, analysis of Justice Sotomayor's hypothesis becomes even more critical.

---

34. *Id.* at 957.
35. *Id*.
36. *See id.* at 954 ("It may be that achieving the same result [as in *Jones*] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.").
37. *See infra* notes 263-87 and accompanying text. This particular issue was not decided in *Jones*, but falls within the types of issues mentioned in *Jones* as likely to receive greater attention. *See Jones*, 132 S.Ct. at 953 ("Situations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis," "but the present case does not require us to answer that question"). *See also id*. at 960 (Alito, J., concurring) ("if long-term monitoring can be accomplished without committing a technical trespass—suppose, for example, that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car—the Court's theory would provide no protection"); *id*. at 955 (Sotomayor, J., concurring) ("With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones.").
38. *See* Julia Angwin, *FBI Turns Off Thousands of GPS Devices After Supreme Court Ruling*, WALL ST. J. BLOGS (Feb. 25, 2012, 3:36 PM), http://blogs.wsj.com/digits/2012/02/25/fbi-turns-off-thousands-of-gps-devices-after-supreme-court-ruling/?mod=WSJBlog (in an article dated February 25, 2012, indicating that the FBI promptly responded to *Jones* by turning off about 3,000 GPS devices that were in use at the time).
39. *See* Timothy B. Lee, *Obama Admin Wants Warrantless Access to Cell Phone Location Data*, ARS TECHNIA (Mar. 8, 2012), http://arstechnica.com/tech-policy/news/2012/03/obama-admin-wants-warrantless-access-to-cell-phone-location-data.ars?utm_source=rss&utm_medium=rss&utm_campaign=rss (in an article dated March 8, 2012, summarizing the Obama administration's position that cell phone "customers have 'no privacy interest' in [cell phone location data] held by a network provider" under the third-party assumption of risk doctrine).

To test Justice Sotomayor's hypothesis, I designed and administered an original empirical study which seeks to uncover the actual views of society on these issues. This survey was administered between October 2011 and February 2012, and resulted in over two hundred responses from individuals of various backgrounds and locations.[40]

The results of my survey are striking. First, my survey results indicate that most respondents would not permit GPS tracking in the absence of a warrant, particularly with respect to the type of suspect at issue in *Jones*, a suspected drug dealer. These results validate the unanimous *Jones* ruling, and empirically demonstrate that the Government's analogy to visual observation of a vehicle in public, as argued in *Jones*, fails to adequately resolve the issue.

Second, my survey results soundly refute *Smith*'s distinction between content and addressing information, a distinction that has been carried forward by analogy to newer forms of communication. Regardless of the particular form of communication at issue, survey respondents did not distinguish between the content and addressing information associated with each identified form of communication. Rather, most respondents believed both types of information should be protected by the Fourth Amendment.

Finally, my survey results refute the assumption of risk rationale underlying *Smith*. Contrary to *Smith*, society today does not believe that a person has no legitimate expectation of privacy in information voluntarily conveyed to third parties, and therefore assumes the risk of disclosure to the government.[41] This evidence strongly supports Justice Sotomayor's hypothesis, and should be considered in cases in which the Government obtains location information directly from a third-party, such as a cell phone provider.[42]

Before summarizing the results of my survey, Part II of this article examines the proper place of analogical reasoning in the judicial decision-making toolkit, and highlights its misapplication in the Fourth Amendment. Part III makes the case for empirical assessments of Fourth Amendment search claims, and argues that the empirical method more accurately accounts for actual expectations of privacy than the analogical reasoning so often employed in cases involving emerging technologies. Part IV sets forth the detailed results of my survey. Part V addresses the impact of my survey results on the warrantless monitoring of a suspect's movements by

---

40. *See infra* Appendix B.

41. *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (citing United States v. Miller, 425 U.S. 435, 442–444 (1976) (holding that a bank depositor has no "legitimate 'expectation of privacy'" in financial information "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business")).

42. This particular issue was not decided in *Jones*, but was mentioned by all nine Justices as an issue likely to be litigated going forward. *See supra* note 37.

third-party cell phone data, which permits the near equivalent of GPS tracking in the absence of a physical trespass, making it the investigative method most likely to be utilized in the wake of *Jones*. Part VI concludes.

II. THE MISAPPLICATION OF ANALOGICAL REASONING IN FOURTH AMENDMENT ANALYSIS

Analogical reasoning as a method of legal analysis works in four simple steps: (1) Some fact pattern, A, is noted for having certain characteristics, such as X, Y, and Z; (2) Fact pattern B differs from A in some respects but shares characteristics X, Y, and Z; (3) The law treats A in a certain way (i.e., the form of surveillance at issue in case A is not considered a Fourth Amendment "search"); (4) Because B shares certain characteristics with A, the law should treat B the same way (i.e., the form of surveillance at issue in case B is also not considered a Fourth Amendment "search").[43]

In Fourth Amendment analysis, analogical reasoning is misapplied in one of two ways: (1) cases are deemed analogous, and therefore deserving of the same outcome, despite relevant differences between the analogized cases; and (2) analogical reasoning is used as a substitute for the case-specific inquiry contemplated by *Katz*. In Fourth Amendment cases, these deficiencies often go hand-in-hand.

In his article *On Analogical Reasoning*,[44] Cass Sunstein recognizes that analogical reasoning, when misapplied, can be the tool that justifies bad outcomes.[45] According to Sunstein, "analogical reasoning can go wrong . . . when some similarities between two cases are deemed decisive with insufficient investigation of relevant differences."[46] When this occurs, "the court has not properly engaged in analogical reasoning."[47] This is the first of two ways in which courts have misapplied analogical reasoning in Fourth Amendment "search" cases, and is particularly apparent in the pre-*Jones* GPS tracking cases.

The second way in which courts have misapplied analogical reasoning in Fourth Amendment analysis is more pervasive in cases involving emerging technologies. In these cases, courts often resort to easy analogies without truly analyzing the precise question presented: *whether the defendant's particular expectation of privacy is one today's society*

---

43. *See* Cass R. Sunstein, *On Analogical Reasoning*, 106 HARV. L. REV. 741, 745 (1993).
44. *See generally* Cass R. Sunstein, *On Analogical Reasoning*, 106 HARV. L. REV. 741 (1993) (defending analogical reasoning as a method of legal analysis while highlighting its flaws).
45. *See id.* at 745 ("analogical reasoning does not guarantee good outcomes or truth").
46. *Id*. at 757.
47. *Id*.

recognizes as reasonable.[48] The fact that society once rejected a defendant's claim of privacy in situation X often says nothing about whether society would likewise reject a defendant's claim of privacy in situation Y. Analogy alone cannot resolve the issue. Otherwise, the actual expectations of privacy would be irrelevant to the analysis, but such an approach would disregard the case-specific nature of the *Katz* test.[49]

If a court resorts to easy analogies without engaging in the case-specific inquiry required by *Katz*, the court is not actually applying the *Katz* test as it has been formulated, and the court's decision may, or may not, accurately reflect society's actual expectations of privacy.[50] Recent Fourth Amendment cases – including GPS tracking, internet and e-mail searches, and text message searches – illustrate this potential flaw in analogical reasoning.

A. GPS Tracking

For years, police departments around the country have been utilizing GPS tracking devices to monitor the movements of criminal suspects without warrants.[51] In the majority of pre-*Jones* GPS tracking cases, courts

---

48. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

49. *See supra* note 18.

50. For an example of an opinion careful to apply the *Katz* test to the particular facts of the case, *see* United States v. Cuevas-Perez, 640 F.3d 272, 274-75 (7th Cir. 2011) (distinguishing an instance of a 28-day GPS tracking from the 60-hour GPS surveillance that occurred in this case).

51. *See, e.g.*, United States v. Wilson, 484 F.3d 267, 281 (4th Cir. 2007) (detailing an extensive federal drug investigation in Maryland involving various investigative techniques, including GPS trackers); United States v. Mayberry, 540 F.3d 506, 511 (6th Cir. 2008) (noting that, as part of their investigation into robberies, police in Michigan "secretly placed a GPS tracking device on the [defendant's] rental car" while it was parked at an apartment complex); United States v. Santiago, 560 F.3d 62, 64-65 (1st Cir. 2009) (detailing "a year-long investigation into a large-scale heroin distribution operation" that occurred in 2003 and 2004 in Massachusetts, in which "agents tracked [defendant's] van with a GPS unit and conducted visual surveillance of it; conducted court authorized wiretaps of cell phones of the defendants; [and] tracked and observed transactions among the defendants revealed by cell phone conversations"); United States v. Pineda-Moreno, 591 F.3d 1212, 1213 (9th Cir. 2010) (noting that "over a four-month period, [DEA] agents [in Oregon] repeatedly monitored Pineda-Moreno's Jeep using various types of mobile tracking devices," and that agents installed the devices on seven different occasions); United States v. Marquez, 605 F.3d 604, 607 (8th Cir. 2010) (recounting how DEA and Iowa state officers placed a GPS tracking device on the bumper of a Ford while it was parked in a Walmart parking lot in Des Moines, Iowa, and subsequently used the device to monitor the vehicle's movements back and forth to Colorado); United States v. Smith, 387 F. App'x. 918, 919 (11th Cir. 2010) (per curiam) (unreported) (describing an investigation in Florida in which police installed a GPS device on the truck of a person suspected of trafficking marijuana); *Cuevas-Perez*, 640 F.3d at 272-73 (describing an investigation in which Arizona police attached a GPS tracking device to the suspect's Jeep which was programmed to send text message updates of the Jeep's location every

concluded that when a GPS device is used to monitor a vehicle's movements in public, the defendant cannot reasonably expect privacy in those movements.[52] In those cases, courts analogized GPS tracking to one of two Supreme Court cases from the early 1980's, each involving the tracking of a vehicle by electronic beeper.

1. The Earlier Era Precedents: Knotts *and* Karo

In *United States v. Knotts*,[53] the first of the Supreme Court's electronic beeper cases, the Court rejected the defendant's Fourth Amendment challenge[54] and upheld the warrantless use of a beeper to track a drum of chloroform from the defendant's point of purchase to a cabin about 100 miles away.[55] According to the Court, the use of the beeper did not constitute a "search" because the beeper did not provide any information police could not have obtained through visual surveillance along the vehicle's route.[56]

Just one year after *Knotts*, the Court, in *United States v. Karo*,[57] examined a similar case and reached the opposite result as in *Knotts*, primarily because the electronic beeper in that case was used to track a can of ether inside a private residence.[58] Distinguishing the public surveillance

---

four minutes, then tracked the Jeep's movements into several states, eventually leading to the suspect's arrest in Illinois).

52. *See, e.g.*, *Pineda-Moreno*, 591 F.3d at 1216-17 (invoking *Knotts* and holding that the GPS tracking of an individual's movements in his vehicle over a prolonged period is not a search); United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007) (relying on *Knotts* and holding that GPS tracking is not a search); *Marquez*, 605 F.3d at 610 ("[w]hen police have reasonable suspicion that a particular vehicle is transporting drugs, a warrant is not required when, while the vehicle is parked in a public place, they install a non-invasive GPS tracking device on it for a reasonable period of time"). *See Cuevas-Perez*, 640 F.3d at 276 (Flaum, J., concurring) ("The practice of using [GPS tracking] devices to monitor movements on public roads falls squarely within the [Supreme] Court's consistent teaching that people do not have a legitimate expectation of privacy in that which they reveal to third parties or leave open to view by others").

53. 460 U.S. 276 (1983).

54. *See id*. at 284-85.

55. Having suspected Knotts of manufacturing drugs, federal officers, without a warrant, had installed a beeper in a chemical drum they knew would be sold to Knotts. With the beeper's assistance, officers followed Knotts's vehicle to where it stopped outside a certain cabin. Based on this information, the police secured a warrant to search the cabin, and uncovered incriminating evidence inside. *Id*. at 278-79.

56. According to the *Knotts* Court, "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," and the "use of the beeper to signal the presence of [the vehicle] . . . does not alter the situation." *Id*. at 282.

57. 468 U.S. 705 (1984).

58. Because the beeper in *Karo* was used to monitor the can's movements within a private residence, *see id*. at 714, the Court described the issue as follows, "whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence." *Id.* at 714.

in *Knotts*, the Court reasoned that "indiscriminate monitoring of property that has been withdrawn from public view" must remain subject to Fourth Amendment oversight.[59]

Invoking *Knotts* and distinguishing *Karo*, pre-*Jones* GPS tracking cases typically concluded that when a GPS device is used to monitor a suspect's movements in public, the suspect cannot reasonably expect privacy in those movements.[60] Applying this inside/outside distinction, pre-*Jones* GPS cases reasoned that GPS tracking is more akin to "non-search" forms of surveillance, such as an officer following a car or tracking a car's movements by means of cameras mounted on lampposts.[61] A minority of pre-*Jones* courts recognized that this rationale, while plausible on its face, does not account for inherent differences between tracking a vehicle for a few hours by beeper and tracking that same vehicle for a substantially longer period of time by GPS.[62] The Court granted certiorari in *Jones* to resolve the split.[63]

---

59. As the Court explained, "[*Karo*] is thus not like *Knotts*, for there the beeper told the authorities nothing about the interior of Knotts' cabin. . . . [H]ere, [by contrast] the monitoring indicated that the beeper was inside the house, a fact that could not have been visually verified [by the police from outside the house]," *id*. at 715, and one that "the Government is extremely interested in knowing." *Id*.

60. *See, e.g.*, United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010) (invoking *Knotts* and holding that the GPS tracking of an individual's movements in his vehicle over a prolonged period is not a search); United States v. Garcia, 474 F.3d 994 (7th Cir. 2007) (same); United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010) (stating in dicta that "[w]hen police have reasonable suspicion that a particular vehicle is transporting drugs, a warrant is not required when, while the vehicle is parked in a public place, they install a non-invasive GPS tracking device on it for a reasonable period of time").

61. Without citing any case law to support its analogy, the Seventh Circuit in *Garcia* viewed GPS tracking as more akin to hypothetical practices it assumed are not searches, such as tracking a car "by means of cameras mounted on lampposts or satellite imaging." *See Garcia*, 474 F.3d 994 ("if police follow a car around, or observe its route by means of cameras mounted on lampposts or of satellite imaging as in Google Earth, there is no search").

62. *See, e.g.*, United States v. Maynard, 615 F.3d 544, 555-68 (D.C. Cir. 2010) (holding that the use of a GPS tracking device to monitor an individual's movements over a four-week period is a search, and rejecting the Government's argument, based on an attempted extension of *Knotts*, that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another" even in such extended instances of GPS tracking); People v. Weaver, 12 N.Y.3d 433, 440–44 (2009) (distinguishing *Knotts*, and declaring "[a]t first blush, it would appear that *Knotts* does not bode well for Mr. Weaver, for in his case, as in *Knotts*, the surveillance technology was utilized for the purpose of tracking the progress of a vehicle over . . . predominantly public roads and, as in *Knotts*, these movements were at least in theory exposed to 'anyone who wanted to look.' This, however, is where the similarity ends.").

63. United States v. Jones, 131 S.Ct. 3064 (2011).

2. The Misapplication of Analogical Reasoning in the GPS Tracking Cases

In *Jones*, all nine Justices of the United States Supreme Court struck down one instance of GPS tracking[64] in which a suspect's vehicle was monitored for 28 days without a warrant.[65] The Court's unanimous agreement as to the result, despite disagreement as to the rationale, highlights critical flaws in the analogical reasoning employed by pre-*Jones* courts.

In *Jones*, officers installed a GPS tracking device on suspect Antoine Jones's jeep while it was parked in a public parking lot.[66] Although the officers had obtained a warrant authorizing installation of the device, the device was installed after the warrant had expired and outside the jurisdiction specified in the warrant.[67] Over the next twenty-eight days, the Government used the device to track the movements of Jones's vehicle.[68] The resulting GPS data connected Jones to a structure that contained large amounts of cash and cocaine.[69]

Jones was then charged with various crimes, including charges related to cocaine possession and distribution.[70] Before trial, Jones unsuccessfully moved to suppress the evidence obtained through the GPS device.[71] Applying *Knotts*,[72] and following most prior GPS-tracking decisions,[73] the trial court reasoned that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements

64. *See* United States v. Jones, 132 S.Ct. 945, 949 (2012) (holding that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a [Fourth Amendment] 'search,'" thereby presumptively requiring a warrant). *See also id*. at 964 (Alito, J., concurring) (concluding on behalf of Justices Alito, Ginsburg, Breyer, and Kagan that the lengthy GPS monitoring that occurred in that case constituted a Fourth Amendment "search," thereby presumptively requiring a warrant); *id*. at 954 (Sotomayor, J., concurring) (agreeing with the majority that "a search within the meaning of the Fourth Amendment occurs, at a minimum, 'where, as here, the Government obtains information by physically intruding on a constitutionally protected area'").

65. *Id*. at 948.

66. *Id*.

67. *Id*. On appeal to the Supreme Court, the Government conceded noncompliance with the warrant, and instead argued that a warrant was not required. *Id.* at 948 n.1.

68. *Id*. at 948. The device relayed more than two-thousand pages of data regarding the vehicle's movements over the four-week period. *Id.*

69. *Id*. at 949.

70. *Id*. at 948-49.

71. The District Court granted the motion in part, suppressing only the data obtained while the vehicle was parked in the garage adjoining Jones's residence. United States v. Jones, 451 F.Supp.2d 71, 88-89 (D.D.C. 2006).

72. 460 U.S. 276 (1983).

73. *See supra* note 22.

from one place to another."[74] Jones was later convicted and sentenced to life imprisonment.[75]

On appeal, the United States Supreme Court considered "whether the attachment of a Global-Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment."[76] The Court unanimously held that it does.[77]

While all nine Justices in *Jones* agreed that this particular instance of GPS tracking was a search, they did not agree on the rationale. Rather than apply the *Katz* test, the majority, consisting of Justices Scalia, Roberts, Kennedy, Thomas, and Sotomayor,[78] applied the pre-*Katz* physical trespass doctrine.[79] Under this test, the majority reasoned that "a vehicle is an 'effect' as that term is used in the [Fourth] Amendment;"[80] and, in this case, the Government physically trespassed upon Jones's vehicle by attaching the device as it was parked in public.[81] As such, "the Government's *installation* of a GPS device on a target's vehicle, *and its use* of that device to monitor the vehicle's movements, constitutes a 'search.'"[82] Because the warrant had already expired at the time of such installation and use, and because the Government presented no other argument to justify the warrantless monitoring,[83] the evidence obtained by GPS had to be suppressed.[84]

---

74. *Jones*, 451 F.Supp.2d at 88 (citing *Knotts*, 460 U.S. at 281-82).
75. *Jones*, 132 S.Ct. at 949.
76. *Id*. at 948.
77. *Id*. at 949. According to the majority, "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'" *Id*.
78. *Id*. at 948.
79. *See id*. at 949-52. According to the majority, *Katz* did not repudiate the understanding that the Fourth Amendment embodies a particular concern for government trespass upon the areas it enumerates. *See id*. at 950. Rather, "[t]he *Katz* reasonable-expectation-of-privacy test has been added to, but not substituted for, the common-law trespassory test." *Id*. at 950-51. Thus, as the majority saw it, "Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation." *Id*. at 950. However, as the majority clarified, "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Id*. at 953.
80. *Id*. at 949.
81. According to the majority, "by attaching the device to the Jeep, officers encroached on a protected area." *Id*. at 952.
82. *Id*. at 949. In a similar passage, the majority declared, "The Government physically occupied private property [i.e., Jones's vehicle] for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id*.
83. *See id*. at 956 (rejecting the Government's argument that the GPS tracking in that case was reasonable).
84. *See id*.

Crucial to the majority's analysis is the fact that "Jones . . . possessed the Jeep at the time the Government trespassorily inserted the [GPS] device."[85] Taking a different approach, Justice Alito's concurring opinion, joined by Justices Ginsburg, Breyer, and Kagan, employed the *Katz* test to analyze the issue, ignoring the effect of any perceived trespass.[86] According to these four Justices, "the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment."[87] And, while the concurring Justices did not attempt to identify the point at which the GPS tracking became a search, the Justices believed "the line was surely crossed before the 4-week mark."[88] Justice Sotomayor, in her own concurrence, agreed.[89]

In the pre-*Jones* GPS tracking cases, courts typically followed the *Katz* framework employed by the concurring Justices in *Jones*. However, unlike the five Justices who endorsed Justice Alito's *Katz*-based analysis,[90] most lower courts had deemed warrantless GPS tracking permissible under the principle that "[a] person traveling . . . on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,"[91] a principle derived from seemingly similar forms of investigation such as an officer following a car turn-by-turn.[92]

---

85. *Id*. at 952. Indeed, the majority distinguished *Karo* on these grounds because in that case, "Karo accepted the container as it came to him, beeper and all, and therefore was not entitled to object to the beeper's presence, even though it was used to monitor the container's location" in much the same way as modern-day GPS. *Id*.

86. Justice Alito's concurring opinion described the issue as "[w]hether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." *Id*. at 958 (Alito, J., concurring).

87. *Id*. at 964.

88. *Id*.

89. Justice Sotomayor ratified the rationales of both Justice Scalia's majority opinion and Justice Alito's concurring opinion. Consistent with the majority, Justice Sotomayor declared "that a search . . . occurs, at a minimum, '[w]here, as here, the Government obtains information by physically intruding on a constitutionally protected area." *Id.* at 954-55 (Sotomayor, J., concurring). Consistent with the concurrence, Justice Sotomayor stated, "I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'" *Id*.

90. *See* United States v. Graham, No. RDB-11-0094, 2012 WL 691531, at *7-*9 (D. Md. March 1, 2012) (discussing the various opinions in *Jones*, and concluding that "a five justice majority [of the United States Supreme Court] is willing to accept the principle that government surveillance over time can implicate an individual's reasonable expectation of privacy"). Notably, the *Jones* majority refused to decide the case under *Katz*, but declared that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Jones*, 132 S.Ct. at 953. Thus, the views of the Justices in the *Jones* majority under a *Katz*-based analysis remain to be seen.

91. *See supra* note 22.

92. Without citing any case law to support its analogy, the Seventh Circuit in *Garcia* viewed GPS tracking as more akin to hypothetical practices it assumed are not searches, such as tracking a car "by means of cameras mounted on lampposts or satellite imaging." *See* United States v. Garcia,

As Justice Alito recognizes, these analogies to distinct modes of investigation fail to account for significant differences between the cases. Indeed, all nine Justices agreed, as implicit in their rejection of the Government's argument,[93] that the lower courts' analogy to *Knotts*,[94] which involved relatively unsophisticated electronic monitoring, is an insufficient method for resolving the more complex issue of GPS tracking. Moreover, in misapplying analogical reasoning, the pre-*Jones* GPS cases failed to recognize that tracking a vehicle over an extended period of time is significantly more invasive of privacy than tracking a vehicle for a few hours.[95] For example, in *United States v. Pineda-Moreno*,[96] the Ninth Circuit Court of Appeals, employing *Katz*, rejected a Fourth Amendment challenge to the warrantless attachment and use of a GPS tracking device under circumstances that would offend all nine Supreme Court Justices.[97]

In *Pineda-Moreno*, agents attached and utilized multiple GPS devices to monitor a vehicle's movements over a four-month period, which would have triggered the concerns of the concurring Justices in *Jones* regarding length of surveillance.[98] There was no question in that case that the vehicle

---

474 F.3d 994, 997 ("if police follow a car around, or observe its route by means of cameras mounted on lampposts or of satellite imaging as in Google Earth, there is no search").

93. In its brief in *Jones*, the United States argued that individuals have no reasonable expectation of privacy in information that is knowingly exposed to public view, and that Jones himself had no reasonable expectation of privacy in the movements of his vehicle on public streets because that information was exposed to public view. *See* Brief for Petitioner at 18 & 38, United States v. Jones, 132 S.Ct. 945 (2012) (No. 10-1259), 2011 WL 5094951.

94. In its brief in *Jones*, the United States analogized this case to *Knotts*, but the majority in *Jones* rejected that argument. *See Jones*, 132 S.Ct. at 952. According to the Government's argument, "[t]his case, like *Knotts*, involves movements of a vehicle on public streets. That location information was 'conveyed to anyone who wanted to look.'" Brief for Petitioner at 22, United States v. Jones, No. 10-1259, 2012 WL 171117 (2012) (No. 10-1259), 2011 WL 5094951. As the Government argued, "*Knotts* was not based on the length of time the beeper was in place or the quantity of information it transmitted to police," but instead "rested on the principle that 'when [the driver] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination.'" Brief for Petitioner at 28, *Jones*, No. 10-1259, 2012 WL 171117 (quoting *Knotts*, 460 U.S. at 281-82).

95. This assertion is supported by Justice Alito's concurrence in *Jones*. In complaining of the majority's trespass-based rationale, Justice Alito wrote that "the Court's reasoning largely disregards *what is really important* (the *use* of a GPS for the purpose of *long-term tracking*)." *Jones*, 132 S.Ct. at 961 (Alito, J., concurring) (first and third emphases added). This rationale applies with equal force to the pre-*Jones* lower court GPS cases that discounted the length of surveillance.

96. 591 F.3d 1212 (9th Cir. 2010).

97. *See id.* at 1214-17 (rejecting arguments based both on the attachment and the use of the device to monitor the vehicle's movements).

98. *See Jones*, 2012 WL 171117, at *17 (Alito, J., concurring) ("the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period"); *id.* at 955 (Sotomayor, J., concurring) (agreeing with the four Justices who joined Justice

belonged to the defendant;[99] moreover, on at least one occasion, the device was attached to the defendant's vehicle while it was parked in the driveway of his residence (and later used to track the vehicle's movements), presumably triggering the *Jones* majority's trespass concerns.[100] For the Supreme Court, this would have been an easy case. Yet, the *Pineda-Moreno* court rejected the defendant's Fourth Amendment challenge by simple analogy to *Knotts*.[101]

Distinctions based upon the length of surveillance are normatively sound; they are also empirically proven by my survey.[102] Under the simple analogy to *Knotts*, warrantless GPS tracking would be permitted to continue indefinitely in the absence of a warrant. However, only 24.2% of my survey respondents were willing to permit warrantless GPS tracking to extend beyond ten days for a suspect similar to Antoine Jones. This evidence indicates that the unanimous *Jones* ruling represents an accurate reflection of society's privacy expectations on this issue.

Normatively speaking, the result should be no different. Unlike the monitoring made possible by today's GPS, which can be accomplished with little to no human interaction,[103] the beeper in *Knotts* emitted periodic

---

Alito's concurrence "that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy'").

99. *See Pineda-Moreno*, 591 F.3d at 1213 (describing defendant Pineda-Moreno as "the owner of the Jeep" and the person seen driving the vehicle).

100. In *Pineda-Moreno*, just as in *Jones*, the GPS tracking device was attached to the suspect's vehicle without the suspect's consent, and the *Jones* majority deemed it significant that "[b]y attaching the device to the Jeep, officers encroached on a protected area." *Jones*, 132 S.Ct. at 952.

101. Regarding the use of the device, the *Pineda-Moreno* court reasoned that "in *Knotts*, as in this case, 'the substitute . . . is for an activity, namely following a car on a public street, that is unequivocally *not* a search within the meaning of the [Fourth] [A]mendment . . . The only information the agents obtained from the tracking devices was a log of the locations where Pineda-Moreno's car traveled, information the agents could have obtained by following the car." *Pineda-Moreno*, 591 F.3d at 1216 (internal citations omitted).

102. *See infra* part IV. Even the *Knotts* Court distinguished between the limited information discovered by use of the beeper in that case— movements during a discrete journey lasting just a few hours—and the sustained monitoring made possible by GPS tracking. Specifically reserving the issue raised in *Jones*, the Court addressed respondent's worry "that 'twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision," by stating that "if such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." United States v. Knotts, 460 U.S. 276, 283-84 (1983). Less explicitly, the *Knotts* Court stated, "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements *from one place to another*." *Id*. at 281 (emphasis added). *See also* People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009) (*Knotts* involved a "single trip" and the *Knotts* Court "pointedly acknowledged and reserved for another day the question of whether a Fourth Amendment issue would be posed if 'twenty-four hour surveillance of any citizen of this country [were] possible'").

103. *See* United States v. Cuevas-Perez, 640 F.3d 272, 275-78 (7th Cir. 2011) (noting that the GPS device used in that case was capable of sending minute-by minute messages to its operator remotely, instead of needing to be physically retrieved like models at issue in earlier cases; further noting that "[a] GPS device works differently than a beeper . . . [a] beeper transmits a signal that a

signals that required simultaneous monitoring by officers situated nearby.[104] Unlike today's GPS, the beeper employed in *Knotts* "amount[ed] to no more than an incremental improvement over following a car by the unassisted eye."[105]

Also distinguished from the electronic beeper in *Knotts*, GPS tracking enables the government to track a suspect's movements twenty-four hours a day for extended periods of time.[106] Discovering the whole of one's movements over such a long time is far more invasive of privacy than discovering one's movements during a single journey, and would be incredibly difficult to replicate through more traditional forms of surveillance.[107] Such prolonged surveillance can allow police to "deduce whether [the suspect] is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."[108] The combination of these observations "tell a story not told by any single visit."[109] Moreover, if *Jones* had deemed this technology exempt from Fourth Amendment

---

receiver can detect. With GPS technology, the unit itself is a receiver: using a process called trilateration, the unit pieces together the geographical coordinates of its location based on its position relative to several orbiting satellites. When affixed to a vehicle, the GPS unit can either record the vehicle's movements for later downloading or transmit the information at intervals. To be sure, GPS units are far more accurate than beepers.") (internal citations omitted).

104. *Knotts*, 460 U.S. at 276. At one time, the trailing officers lost the signal from the beeper, but were able to regain the signal about one hour later. *Knotts*, 460 U.S. at 278.

105. *Weaver*, 12 N.Y.3d at 442.

106. *See supra* note 51.

107. This distinction was recognized by several pre-*Jones* GPS tracking cases. *See* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) ("It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine."); *See Weaver*, 12 N.Y.3d at 440–44 ("Knotts involved the use of . . . a very primitive tracking device. The device was, moreover, used . . . for the discreet purpose of ascertaining the destination of a particular container of chloroform . . . . GPS is a vastly different and exponentially more sophisticated and powerful technology that is easily and cheaply deployed and has virtually unlimited and remarkably precise tracking capability . . . The potential for a similar capture of information or 'seeing' by law enforcement would require . . . millions of additional police officers and cameras on every street lamp").

108. *Maynard*, 615 F.3d at 562. *See also Weaver*, 12 N.Y.3d at 441–42 ("[With GPS tracking], [t]he whole of a person's progress through the world . . . can be charted and recorded over lengthy periods . . . . Disclosed in the data retrieved from the transmitting unit . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on. What the technology yields and records with breathtaking quality and quantity is a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous . . . .")

109. *Id*.

protection, nothing would have prevented police from affixing GPS tracking devices to thousands of cars at random and "using digital search techniques to identify suspicious driving patterns."[110] The potential for privacy invasion in such mass surveillance is vast,[111] and bears little resemblance to trailing a car turn-by-turn.

While *Jones* now forecloses the possibility of "affixing GPS tracking devices to thousands of cars at random,"[112] at least where doing so involves a physical trespass upon the vehicle, *Jones* did not resolve whether similar forms of electronic monitoring would be permissible in the absence of a physical trespass.[113] Yet, five Justices in *Jones*, employing the *Katz*-based analysis that would govern such cases, highlighted the length of surveillance as a critical factor.[114] As these Justices recognized, the length of surveillance,[115] along with the degree of invasiveness inherent in the tracking of one's every movement,[116] will become critical factors in future instances of electronic monitoring accomplished without a physical trespass. Even in these unresolved aspects of electronic monitoring, the *Knotts* principle exempting Fourth Amendment protection from activities knowingly exposed to the public[117] is simply too simplistic to control the outcome.[118]

---

110. United States v. Garcia, 474 F.3d 994, 997-98 (7th Cir. 2007).
111. *See* SLOBOGIN, *supra* note 15 at 90-98 (arguing that mass governmental surveillance would inevitably change behavior and would stifle spontaneity, leading to more measured lives).
112. *Id*.
113. United States v. Jones, 132 S.Ct. 945, 962 (2012) (Alito, J., concurring) ("if long-term monitoring can be accomplished without committing a technical trespass—suppose, for example, that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car—the Court's theory would provide no protection.").
114. *See supra* notes 85-89 and accompanying text.
115. *Jones*, 132 S.Ct. at 964 (Alito, J., concurring) (concluding that "the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment"); *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.'").
116. *See id.* at 955-56 (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 . . . . 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.").
117. *See* United States v. Knotts, 460 U.S. 276, 281-82 (1983) (emphasizing that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another").
118. *See Jones*, 132 S.Ct. at 955 (Sotomayor, J., concurring) ("I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques.").

B. Internet and E-mail Searches

The second exemplary line of cases in which analogical reasoning has failed to accurately reflect society's actual privacy expectations are those involving the Court's distinction between the content of various communications, which are protected by the Fourth Amendment, and the addressing information associated with those communications, which are not.[119] Underlying this distinction is the principle that individuals cannot reasonably expect privacy in information voluntarily disclosed to third parties;[120] so-called "addressing information" often falls within that category.

1. The Earlier Era Precedents: Miller *and* Smith

The assumption of risk doctrine arose in the Court's early *Katz* cases, most notably *United States v. Miller*[121] and *Smith v. Maryland*,[122] and has been extended by analogy to a range of distinct forms of communication.

In 1976, the Court, in *Miller*, held that a bank customer cannot legitimately expect privacy in financial information he "voluntarily conveys" to bank employees in the ordinary course of business.[123] No Fourth Amendment search occurs, therefore, if the bank hands over the customer's financial records to the Government.[124]

In *Miller*, police received a tip indicating that Mitch Miller and others were engaged in the illegal manufacture of whiskey.[125] As part of their investigation, federal agents presented subpoenas to two banks where Miller kept accounts.[126] The subpoenas, later deemed faulty,[127] required the banks to produce "all records of accounts, i.e., savings, checking, loan or otherwise, in the name of Mr. Mitch Miller" over a four-month period.[128]

---

119. *See* Smith v. Maryland, 442 U.S. 735, 743 (1979) ("Although petitioner's conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.").
120. *See id*.
121. 425 U.S. 435 (1976).
122. 442 U.S. 735 (1979).
123. *Miller*, 425 U.S. at 442.
124. As the Court stated, "no Fourth Amendment interests of the depositor are implicated here." *Id*. at 444.
125. *See id*. at 436 (setting forth the charges eventually brought against Miller).
126. *Id*. at 437.
127. According to the Court of Appeals, "a purported grand jury subpoena, issued not by the court or by the grand jury, but by the United States Attorney's office, for a date when no grand jury was in session, and which in effect compelled broad disclosure of Miller's financial records to the government, does not constitute sufficient 'legal process'. . . ." United States v. Miller, 500 F.2d 751, 757-58 (5th Cir. 1974).
128. *Miller*, 425 U.S. at 437.

The banks complied with the request by furnishing copies of checks, deposit slips, and financial statements.[129]

Miller subsequently argued that the bank documents were illegally seized, and sought to suppress those documents.[130] The district court denied Miller's motion, but the Fifth Circuit Court of Appeals reversed.[131] According to the Fifth Circuit, *Boyd v. United States*[132] "determined . . . that 'a compulsory production of a man's private papers to establish a criminal charge against him . . . is within the scope of the Fourth Amendment,'"[133] and "[t]he government may not cavalierly circumvent *Boyd*'s precious protection by first requiring a third party bank to copy all of its depositors' personal checks [by statute] and then, with an improper invocation of legal process, calling upon the bank to allow . . . reproduction of those copies."[134]

On further appeal, the United States Supreme Court disagreed. Distinguishing *Boyd*, the Court reasoned that "the documents subpoenaed here are not [Miller's] 'private papers.' . . . Instead, these are the business records of the banks."[135] Moreover, "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[136] This, according to the Court, is true "even if the information is revealed on the assumption that it will be used only for a limited purpose . . . ."[137] As such, the Court concluded that Miller "possessed no Fourth Amendment interest that could be vindicated," and therefore could not suppress the evidence obtained from the bank.[138]

Three years after *Miller*, the Court extended *Miller*'s assumption of risk rationale in *Smith v. Maryland*.[139] The events in *Smith* began when Baltimore resident Patricia McDonough was robbed.[140] McDonough gave the police a description of the robber and of a 1975 Monte Carlo automobile she had observed near the crime scene.[141] McDonough soon began receiving threatening phone calls from a man identifying himself as

---

129. *See id.* at 438.
130. *Id*. at 438-39.
131. United States v. Miller, 500 F.2d 751, 756 (5th Cir. 1974). The Fifth Circuit concluded that "obtaining copies of Miller's bank checks by means of a faulty subpoena . . . constituted an unlawful invasion of Miller's privacy, and that any evidence so obtained should have been suppressed." *Id.*
132. 116 U.S. 616 (1886).
133. *Miller*, 500 F.2d at 757.
134. *Id.*
135. *Miller*, 425 U.S. at 440.
136. *Id.* at 443.
137. *Id.*
138. *Id.* at 445.
139. 442 U.S. 735 (1979).
140. *Id*. at 737.
141. *Id*.

the robber.[142] Police then spotted a man who met the description offered by McDonough driving a 1975 Monte Carlo in her neighborhood,[143] and discovered that the car was registered to Michael Lee Smith.[144]

Without a warrant,[145] police requested the local telephone company to install a pen register on telephone company property, which was used to record the phone numbers dialed from Smith's home.[146] Once installed, the pen register revealed that a call was placed from Smith's home to McDonough's phone several days after the robbery.[147] With this evidence, police obtained a warrant to search Smith's residence,[148] which subsequently revealed that a page in Smith's phone book had been turned down to the name of Patricia McDonough.[149]

Before Smith's robbery trial, Smith moved to suppress "all fruits derived from the [warrantless use of the] pen register," which included the phone book recovered from Smith's home and the list of phone numbers he had dialed.[150] The trial court denied Smith's motion,[151] and Smith was convicted.[152]

On appeal, the Supreme Court considered whether the installation and use of a pen register constitutes a Fourth Amendment "search."[153] Applying the *Katz* test,[154] the Court first considered whether Smith had a subjective expectation of privacy regarding the numbers he dialed on his phone. Distinguishing the content of telephone conversations from the numbers dialed, the Court reasoned that "[a]lthough [Smith]'s conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number[s] he dialed."[155] According to the Court, "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that

142. *Id*.
143. *Id*.
144. *Id*.
145. *Id*.
146. *Id*. As the Court explained, a pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial of the telephone is released. It is usually installed at a central telephone facility and records on paper tape all numbers dialed from the line to which it is attached. *Id*. at 736 n.1.
147. *Id*. at 737.
148. *Id*.
149. *Id*.
150. *Id*.
151. *Id*. at 737-38.
152. *Id*. at 738.
153. *Id*. at 736.
154. *See id*. at 740 (setting forth the two-part inquiry required by *Katz*).
155. *Id*. at 743.

their calls are completed."[156] Moreover, "[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."[157] For these reasons, "telephone subscribers [do not] . . . harbor any [actual] expectation that the numbers they dial will remain secret."[158] These general expectations among society, according to the Court, make it highly unlikely that Smith himself actually expected privacy in the numbers dialed from his phone.

Next, the Court concluded that "even if [Smith] did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as reasonable.'"[159] Citing *Miller*, along with the Court's participant monitoring cases,[160] the Court invoked the principle that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[161] Analogizing the case to *Miller*, who could not reasonably expect his financial records to remain private once they had been revealed to the bank,[162] the Court reasoned that when Smith used his phone, he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business," and that equipment "is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber."[163] As a result, Smith "assumed the risk that the company would reveal to police the numbers he dialed."[164] For these reasons, the Court concluded that "[t]he installation and use of [the] pen register . . . was not a 'search,' and no warrant was required."[165]

---

156. *Id*. at 742.
157. *Id*.
158. *Id*. at 743.
159. *Id*.
160. Here, the Court cited United States v. White, 401 U.S. 745 (1971) (holding that a person cannot reasonably expect that a person with whom he is conversing will not reveal the conversation to the police because, by speaking, a person knowingly exposes his thoughts to another and to the police), and Hoffa v. United States, 385 U.S. 293 (1967) (finding no Fourth Amendment "search" when defendant Hoffa conversed with his acquaintance in Hoffa's hotel suite, reasoning that we "assume the risk" that a "friend" will betray us; according to the Court, Hoffa "was not relying on the security of the hotel room; he was relying upon his misplaced confidence that [FF] would not reveal his wrongdoing.").
161. *Smith*, 442 U.S. at 743-44.
162. *See id.* at 744.
163. *Id*.
164. *Id*.
165. *Id.* at 745-46.

2. The Misapplication of Analogical Reasoning in Internet and E-mail Cases

In the last forty years, *Miller* and *Smith* have been repeatedly cited for the proposition that "[i]ndividuals who convey information to third parties have 'assumed the risk' of disclosure to the government."[166] Justice Sotomayor questioned this assumption in *Jones*, and doubted "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."[167] As set forth in Part IV, my survey results empirically verify Justice Sotomayor's concerns. Contrary to *Smith*, society today does not believe that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and therefore "assumes the risk" of disclosure to the government.[168] Of the 216 individuals completing this question, 186 respondents, or 86.1%, believed police should have to obtain a warrant before accessing private information conveyed to a bank, a phone company, or any other third-party organization.

Analogies to *Miller* and *Smith* are not only empirically inaccurate; they are also flawed substitutes for the case-specific inquiry required by *Katz*. *United States v. Forrester*[169] exemplifies how courts have misused analogical reasoning to sidestep the requisite *Katz* inquiry in cases involving internet and e-mail searches.

In *Forrester*, defendants Mark Forrester and Dennis Alba were charged with various offenses relating to the operation of an Ecstasy-manufacturing laboratory.[170] During its investigation of Forrester and Alba, the Government received court permission to install a device known as a "mirror port" on Alba's account with PacBell Internet.[171] The mirror port was installed on PacBell property, and enabled the Government to learn the to/from addresses of Alba's e-mail messages, the Internet protocol

166. *Id*. at 749 (Marshall, J., dissenting).
167. United States v. Jones, 132 S.Ct. 945, 954 (2012) (Sotomayor, J., concurring).
168. *See Smith*, 442 U.S. at 743-44 (citing United States v. Miller, 425 U.S. 435, 442-44 (1976)).
169. 512 F.3d 500 (9th Cir. 2007).
170. Forrester and Alba were indicted on October 26, 2001. Both Alba and Forrester were charged with one count of conspiracy to manufacture and distribute Ecstasy in violation of 21 U.S.C. §§ 841(a)(1), 846. Alba was additionally charged with engaging in a continuing criminal enterprise in violation of 21 U.S.C. § 848(a), conspiracy to transfer funds outside the United States in promotion of an illegal activity in violation of 18 U.S.C. § 1956(a)(2)(A)(i), (h) and conspiracy to conduct financial transactions involving the proceeds of an illegal activity in violation of 18 U.S.C. § 1956(a)(1)(A)(i), (h). Both defendants pleaded not guilty to all charges. *Forrester*, 512 F.3d at 505.
171. *Id*.

(IP) addresses of the websites that Alba visited, and the total volume of information sent to or from his account.[172]

After a jury trial, Forrester and Alba were convicted on all counts and received lengthy prison sentences.[173] On appeal, Alba challenged the validity of the Government's warrantless computer surveillance.[174] Rejecting Alba's appeal, the Ninth Circuit Court of Appeals held that police use of computer surveillance to reveal "to" and "from" addresses of e-mail messages sent and received and addresses of websites visited was not a Fourth Amendment "search."[175] Analogizing the case to *Smith v. Maryland*,[176] the Ninth Circuit reasoned that both the pen register and the internet/e-mail address search are distinguishable from more intrusive techniques in that neither technology acquires the contents of the communication at issue; rather, each technology reveals only the addressing information associated with the particular communication.[177] Moreover, by voluntarily conveying the addressing information at issue to a third-party provider, the user relinquished all expectations of privacy in that information.[178]

Under the *Forrester* rationale, when a defendant exposes his otherwise private information to a third party internet service provider, the defendant is presumed to have exposed that information to law enforcement. This argument, while a plausible extension of *Smith*, does not honor the case-specific nature of the *Katz* test.[179] The fact that society in 1979 presumably rejected Smith's privacy claim in the phone numbers dialed from his home phone says nothing about whether society in the year 2007 (the year *Forrester* was decided) would likewise reject Alba's expectation of privacy. Analogies between the cases can easily be made, but analogies are an

---

172. *Id*. Later, the government obtained a warrant authorizing it to employ imaging and keystroke monitoring techniques, but Alba did not challenge the legality of those techniques. *Id*. at 505-06.
173. *Id*. at 506.
174. *Id.* at 504.
175. *Id.* at 510.
176. 442 U.S. 735 (1979).
177. *Forrester*, 512 F.3d at 510. This ruling rests upon the potential distinction, noted by the Ninth Circuit and applied by subsequent courts, between monitoring IP addresses of websites visited (which arguably do not "reveal content") and monitoring the URL's of the pages visited (which reveal significantly more content by identifying the particular document within a website that a person views). A surveillance technique that captures IP addresses would show only that a person visited the New York Times' website at http://nytimes.com, whereas a technique that captures URL's would also divulge the particular articles the person viewed. *See* Doe v. Prosecutor, Marion Cnty., Ind., 566 F.Supp.2d 862, 880 n.6 (S.D. Ind. 2008).
178. *See Forrester*, 512 F.3d at 510 ("Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.").
179. *See supra* note 18 and accompanying text.

imperfect substitute for the case-specific inquiry required by *Katz*. Moreover, the assumption of risk rationale, when applied reflexively to new technologies, disregards potential distinctions in the risks we can fairly be said to assume in modern society. Because people in modern society have virtually no choice but to use internet and e-mail communications as part of their daily lives,[180] privacy in one's e-mail and internet communications should not be considered "a discrete commodity, possessed absolutely or not at all."[181] If a person discloses information to a third-party internet, e-mail, or telephone provider in the ordinary course of using those technologies to carry out daily tasks, it does not necessarily follow that the individual assumes the risk that this information will then be disclosed to other entities for other purposes.[182] If that were true, then the distinction between content and addressing information would not make sense, as both content and addressing information are each routinely conveyed to third party providers.

In contrast to *Forrester*, courts analyzing the warrantless police access of the *content* of one's e-mails[183] have more readily recognized the inability of analogical reasoning to account for relevant differences in distinct forms

---

180. *See* Untied States v. Jones, 132 S.Ct. 945, 959 (2012) (Sotomayor, J., concurring) (questioning the continued validity of the third party assumption of risk doctrine as "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," and declaring, "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"). *Cf.* Burrows v. Super. Ct., 13 Cal.3d 238, 247 (Cal. 1974) (rejecting *Smith*'s assumption of risk rationale under the relevant provisions of the California State Constitution, and noting that "[f]or all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account;" while limiting its analysis to warrantless police access of bank statements, the *Burrows* court further noted that "the logical extension of the contention that the bank's ownership of records permits free access to them by any police officer extends far beyond such statements to checks, savings, bonds, loan applications, loan guarantees, and all papers which the customer has supplied to the bank to facilitate the conduct of his financial affairs upon the reasonable assumption that the information would remain confidential.").

181. *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

182. A variety of prominent scholars have advanced this argument over the past several decades. *See, e.g.*, Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1086 (2002); RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 140 (2006); Sherry F. Colb, *What Is A Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002).

183. As used here, "content" refers to the message body of the e-mail. The other fields, which assist in e-mail transfer from sender to recipient, are considered addressing information for purposes of the Fourth Amendment. Examples of these attributes are the "to" address, the "from" address, the sender's and receiver's IP addresses, and the time and date stamp. Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 611-13 (2003).

of communication. In *Warshak v. United States*,[184] for example, the United States Court of Appeals for the Sixth Circuit analyzed in dicta whether a Fourth Amendment search occurs when the Government accesses e-mail contents.[185] In that case, the Government sought to obtain from Steven Warshak's internet service provider—without a warrant, without probable cause, and without Warshak's knowledge—the contents of Warshak's e-mails that had been "accessed, viewed, or downloaded" more than 180 days prior to the request.[186] The Government obtained authorization for the search from a magistrate judge, but the order was based upon a standard less demanding than probable cause (as authorized by the controlling statute, Section 2703(d) of the federal Stored Communications Act).[187]

When Warshak learned about the orders roughly one year later, he filed a declaratory judgment action seeking to invalidate Section 2703(d) of the Stored Communications Act as facially violative of the Fourth Amendment.[188] According to Warshak, the statute violated the Fourth Amendment because it authorized e-mail searches on less than probable cause and without warrants.[189] Agreeing with Warshak, the district court ruled that internet users reasonably expect privacy in the contents of their e-mails, and that the statute's authorization of searches on less than probable cause contravened the Fourth Amendment.[190]

---

184. Warshak v. United States, 532 F.3d 521 (6th Cir. 2008) (en banc).

185. *See id.* at 526-31.

186. The Government's request was made pursuant to subsection (d) of the federal Stored Communications Act, 18 U.S.C. § 2703. This statute describes when and how the government may compel "a provider of electronic communication service" to disclose "the contents of an electronic communication, that is in electronic storage." 18 U.S.C. § 2703(a) (2006). The statute provides differing levels of protection to different types of e-mail. For e-mails stored 180 days or less, the statute requires warrants and probable cause to compel disclosure. 18 U.S.C. § 2703(a). However, the Government may compel disclosure of e-mails stored on a server for more than 180 days by satisfying a standard of reasonable suspicion without the need for a warrant; under this portion of the statute, the government may compel disclosure of e-mails without a warrant if the government gives the subscriber prior notice and obtains either an administrative subpoena or court order based on "specific and articulable facts showing that there are reasonable grounds to believe that the contents of [the] communication . . . are relevant and material to an ongoing criminal investigation." *See* 18 U.S.C. §§ 2703(b)(1)(B), 2703(d). Additional provisions allow the Government to delay notice to the subscriber for up to ninety days. 18 U.S.C. §§ 2703(b)(1)(B), 2705(a)(1)(A) (2006).

187. *See* 18 U.S.C. § 2703(d) (providing that "[a] court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.").

188. Warshack, 532 F.3d at 522.

189. *Id*. at 524.

190. *Id*. at 525. Warshak was eventually prosecuted and convicted on 93 counts of bank fraud, mail fraud, and money laundering, among other federal crimes. *Id*. at 525.

On appeal, the Sixth Circuit Court of Appeals did not reach the merits of Warshak's claim because it ruled that his claim was not ripe for adjudication.[191] However, the court described the underlying issue as follows: "In permitting the government to search e-mails based on 'reasonable grounds,' is [Section 2703(d) of the Stored Communications Act] consistent with the Fourth Amendment, which generally requires 'probable cause' and a warrant in the context of searches of individuals, homes and, perhaps most analogously, posted mail?"[192]

Had the Sixth Circuit followed the *Forrester* approach, the court would have simply invoked the noted analogy to "posted mail," which generally receives Fourth Amendment protection,[193] and would have presumably found a legitimate expectation of privacy in e-mail as well. Instead, the court sought to determine whether Warshak could reasonably expect privacy in the contents of his e-mails, a question that would depend on the unique facts of the case. According to the court, whether an individual can reasonably expect privacy in the contents of one's e-mail is inherently case-specific, and "assuredly shifts from internet-service agreement to internet-service agreement."[194] For example, an agreement might specify that e-mails will be provided to the government on request, as Warshak's Yahoo! account did.[195] An agreement might also state that the user has no expectation of privacy in any of her communications.[196]

Notably absent from the *Warshak* court's analysis is any reference to expectations of privacy in the contents of posted mail. The *Warshak* court correctly disregarded the potential analogy. If asserted expectations of privacy in one's e-mail turn on "the variety of internet-service agreements and the differing expectations of privacy that come with them," and if those agreements can change over time, then it would be too simplistic to resolve this complex issue by reference to the privacy expectations attached to posted mail. Indeed, while e-mail and regular mail are similar in some

---

191. *See id*. at 525-34.
192. *Id*. at 526.
193. Regular mail is protected by the Fourth Amendment, and generally may not be opened in the absence of a warrant. *See* Olmstead v. United States, 277 U.S. 438, 464 (1928) ("It is plainly within the words of the [Fourth] [A]mendment to say that the unlawful rifling by a government agent of a sealed letter is a search and seizure of the sender's papers of effects."); Ex Parte Jackson, 96 U.S. 727, 733 (1877) ("Letters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. . . . Whilst in the mail, they can only be opened and examined under like warrant . . . .").
194. *Warshak*, 532 F.3d at 526-27.
195. *Id*. at 527.
196. *Id*.

ways,[197] they are entirely distinct forms of communication—one physical and one digital—and the expectations of privacy we attach to each might differ depending on a variety of case-specific factors.

Factors that may alter expectations of privacy in e-mail include the potentially large number and type of recipients involved; statutes, like the Wiretap Act, that prohibit the interception of e-mail by law enforcement and Internet Service Provider (ISP) employees; individual policies of ISP's, which may either treat e-mail as confidential or may warn users that e-mail is subject to monitoring;[198] whether the particular e-mail server is web-based;[199] and even simple e-mail delivery settings.[200] Additional factors

---

197. For example, both forms of communication are used to transmit ideas between people. 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, 200 (2010).

198. *See id.* at 205-06 (examining several factors that might create a reasonable expectation of privacy in the interception of e-mails during transmission, including (1) federal statutes, like the Wiretap Act, that prohibit the interception of e-mail by law enforcement and Internet Service Provider (ISP) employees; (2) policies of ISP's, many which treat customer e-mail as confidential; and (3) the fact that e-mail messages afford a similar level of security associated with other communication devices, such as telephones and letters, in which reasonable expectations of privacy exist). Courts that have rejected asserted expectations of privacy in e-mail have often emphasized the type of e-mail used, including whether the e-mail is sent on a public network; the number and type of recipients involved; and any particular warning or policy regarding guarantees of privacy. *See, e.g.*, Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (ruling that Internet bulletin board users could not legitimately expect privacy in materials posted to a public Internet bulletin board where a posted disclaimer stated that personal communications were not private); United States v. Charbonneau, 979 F.Supp. 1177, 1183-85 (S.D. Ohio 1997) (discussing expectations of privacy in e-mail, and concluding "[t]he expectations of privacy in e-mail transmissions depend in large part on both the type of e-mail sent and recipient of the e-mail," and noting that "[e]-mail messages sent to an addressee who later forwards the e-mail to a third party do not enjoy the same reasonable expectations of privacy once they have been forwarded"); United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000) (finding no expectation of privacy in e-mail in a system owned by the Government which included a specific notice that "users logging on to this system consent to monitoring," and where "the provider of electronic communications service, in this case the Air Force . . . , is specifically exempted from any statutory liability for unlawful access to stored electronic communications").

199. *See* Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U. L. REV. 1043, 1044-61 (2008) (explaining, through hypotheticals, that "181 days after receiving an e-mail, a recipient using an e-mail client set to POP [Post Office Protocol] will have full Fourth Amendment protection while a recipient using either an e-mail client set to IMAP [Internet Message Access Protocol] or a web-based client [such as Google mail] will not").

200. *See id.* As compared to interception of an e-mail during transmission, which may or may not trigger privacy concerns, courts have generally ruled that an e-mail sender loses any expectation of privacy in an e-mail once it reaches its recipient; at this moment, the e-mail is analogous to a letter which is private when sealed but may be shared with others once received by the recipient. *See, e.g.*, Commonwealth v. Proetto, 771 A.2d 823, 829 (Pa. Super. Ct. 2001) (finding no reasonable expectation of privacy in e-mail messages sent by a man to a 15-year-old girl where the girl had forwarded those messages to detectives; moreover, because "there was no contemporaneous acquisition of the communication" by the government, there was no "interception," making these communications exempt from the controlling federal and state statutes).

implicating other constitutional concerns might also be significant.[201] These factors, most of which do not apply to regular mail, may easily generate differing expectations of privacy in the two forms of communication.[202] Thus, analogizing e-mail to regular mail, without examining the factors that would impact privacy expectations as to each, threatens to distort the issue.

C. Text Message Searches

As in *Warshak*, the Supreme Court in *Ontario v. Quon*[203] implicitly recognized the inability of analogical reasoning to adequately resolve a sophisticated *Katz* claim. In that case, police officer Jeff Quon sued his employer, the City of Ontario, alleging that the police department violated the Fourth Amendment by surreptitiously reviewing text messages sent and received on his employer-owned pager.[204]

Although the Court treated the *Katz* issue as superfluous to its decision, the Court noted a variety of case-specific factors that would influence the analysis. The Court stated, for example, that "many employers . . . tolerate personal use of [cell phones] because it often increases worker efficiency",[205] that some States have statutes governing such employee-monitoring;[206] and that clearly communicated employer policies will shape employee expectations.[207] Moreover, the Court noted that it would be necessary to explore stated workplace policies, including "whether [Quon's supervisor] had . . . authority to make . . . a [policy] change."[208] The Court further declared that "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means . . . for self-expression," which "might strengthen the case for an expectation of privacy."[209] On the other hand, the Court noted, "the ubiquity of those devices has made them generally affordable, so one

201. For example, a court deciding a claim such as Warshak's might require warrants simply to avoid the "chilling effect" that failure to do so might create (albeit under a different constitutional right). *See Warshak*, 532 F.3d at 533 (discussing this potential argument, but rejecting the claim because Warshak did not challenge the government's action on First Amendment grounds).

202. *See* Ray, *supra* note 197, at 181-82 (noting that "courts have long held that the content of sealed mail is subject to the Fourth Amendment's protections;" however, "many courts have refused to recognize e-mail users' expectations of privacy").

203. City of Ontario v. Quon, 130 S.Ct. 2619 (2010).

204. *Id.* at 2626.

205. *Id.* at 2629.

206. *Id.* at 2630.

207. *Id.*

208. *Id.* at 2629.

209. *Id.* at 2630.

could counter that employees who need [such] devices for personal matters can purchase and pay for their own."[210]

As the *Quon* Court recognized, a variety of case-specific factors would impact expectations of privacy in the contents of one's text messages. Nowhere within the opinion does the Court analogize the case to similar forms of communication of an earlier technological era, nor should it. After all, the case-specific inquiry contemplated by *Katz* would be undermined by analogizing text messages to a potential physical substitute, such as handwritten notes, because expectations of privacy in each form of communication would be shaped by entirely different factors. When sophisticated technologies present difficult Fourth Amendment issues, courts should not substitute simplistic analogies for actual analysis.

III. EMPIRICAL ASSESSMENTS OF FOURTH AMENDMENT CLAIMS

Imagine a world in which the *Katz* test was adopted in the year 2012, rather than 1967, and in which no *Katz* issues had yet to be decided. Further, imagine a world where the very first *Katz* issue to come before the Court is the issue in *Jones*: "whether the attachment of a Global-Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search . . . within the meaning of the Fourth Amendment."[211]

Without the benefit of analogy to prior *Katz* claims, what would the Court do? If, in this hypothetical world, we were to remove analogical reasoning from the judicial decision-making toolkit, how would the Court decide the case under the freshly minted *Katz* standard? The answer is simple. The Court would follow the explicit mandate of *Katz* and would ask whether "society is prepared to recognize [Jones's asserted privacy expectation] as reasonable."[212] There is no better way to answer that question than to ask society.[213]

---

210. *Id.* After pages of dicta on the issue, the Court eventually assumed, for purposes of analysis, that "Quon had a reasonable expectation of privacy in the text messages [at issue]," and that "[the city's] review of [Quon's text messages] constituted a search within the meaning of the Fourth Amendment." *Id.*

211. United States v. Jones, 132 S.Ct. 945, 947 (2012).

212. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable.'").

213. Scholars agree. *See, e.g.*, SLOBOGIN, *supra* note 15, at 33 (arguing that "some assessment of societal attitudes about the relative intrusiveness of police actions should inform the analysis" under *Katz*, and noting that "the Court has pretty much ignored this precept, with predictably anomalous results"); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting*

As compared to analogical reasoning, empirical evidence is a more accurate indicator of society's actual expectations of privacy in a given case. Taken literally, the *Katz* inquiry anticipates examination of society's actual expectations of privacy and suggests that the Court's practice of deciding Fourth Amendment questions without doing so is a flawed approach.[214]

According to Christopher Slobogin, there are at least two ways to assess societal attitudes about privacy. The first is to examine property, contract, and tort doctrine for clues as to what we think is private.[215] For example, in the context of GPS tracking, the California legislature has made it unlawful for anyone but a law enforcement agency to "use an electronic tracking device to determine the location or movement of a person," and has specifically declared that "electronic tracking of a person's location without that person's knowledge violates that person's reasonable expectation of privacy."[216] Other states have enacted legislation imposing civil and criminal penalties for the use of electronic tracking devices and expressly requiring exclusion of evidence produced by such a device unless obtained pursuant to a warrant.[217]

A second method is to simply pose the question to society.[218] This form of empirical analysis is gaining acceptance among legal scholars. In the Fourth Amendment context, scholars have employed the empirical approach to analyze various "search" issues.[219] My survey particularly follows in the footsteps of similar surveys conducted by Christopher Slobogin.

Through empirical studies, Christopher Slobogin has shown that the Court's *Katz* holdings do not always reflect societal notions of privacy.[220] In 1993, Christopher Slobogin and Joseph Schumacher conducted a survey, completed by 217 individuals, which included fifty scenarios involving

---

Third-Party Information, Third Parties, and the Rest of us Too, 34 PEPP. L. REV. 975, 1000 (2007) ("I part with the High Court . . . on its refusal to determine those expectations [of privacy] in any rational manner. Rather than grapple with the complications of surveys or other evidence, the Court has been content to declare societal expectations without any foundation or support. . . . Either courts should look to academic empirical studies like those done by Professor Slobogin (in which case we need more like them), or litigants should prepare relevant surveys" of their own.).

214. *See* SLOBOGIN, *supra* note 15, at 113-14.

215. *Id*. at 33.

216. CAL. PENAL CODE § 637.7 (West 2012).

217. *See, e.g.*, UTAH CODE ANN. §§ 77-23a-4, 77-23a-7, 77-23a-15.5 (West 2012); MINN. STAT. §§ 626A.37, 626A.35 (2012); FLA. STAT. § 934.42 (2012); S.C. CODE ANN. § 17-30-140 (2012); OKLA. STAT., tit. 13, §§ 176.6, 177.6 (2012); HAW. REV. STAT. §§ 803-42, 803-44.7 (2012); 18 PA. CONS. STAT. § 5761 (2012).

218. SLOBOGIN, *supra* note 15, at 33.

219. *See, e.g.*, *id.* at 112, 184 (tables reporting empirical data).

220. *See id.* at 29 ("the Court's cases defining 'search' for Fourth Amendment purposes have shown no compunction in mutilating that term beyond recognition"). *See also id.* at 112 & 184 (tables reporting empirical data).

various forms of police investigation.[221] Slobogin's second survey was completed by 190 people, and contained twenty scenarios, including various forms of camera surveillance, beepers, and "see-through" devices.[222]

In each of these studies, the subjects were asked to rate each investigative method in terms of "intrusiveness" on a scale of 1 to 100, with 1 representing "not intrusive" and 100 representing "very intrusive."[223] Survey participants[224] were asked to assume that the subject of the search or seizure was innocent,[225] and that the search or seizure was nonconsensual.[226]

Slobogin and Schumacher hypothesized that "many of the Court's conclusions about expectations of privacy and autonomy do not correlate with actual understandings of innocent members of society."[227] The results of their initial survey appear to verify that hypothesis. The relative intrusiveness ratings of three government actions the Court has declared are not searches are particularly instructive: helicopter overflights four hundred feet above the backyard (M = 50),[228] being followed by a police officer (M = 50),[229] and curbside garbage searches (M = 51).[230] These

---

221. Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look At 'Understandings Recognized and Permitted by Society,'* 42 DUKE L.J. 727 (1993).

222. *See* SLOBOGIN, *supra* note 15, at 110-11 (describing survey design).

223. *Id*. at 111. *See also* Slobogin & Schumacher, *supra* note 221, at 735-36. According to Slobogin, "[w]ith respect to searches, we wanted to discover [society's] expectations of privacy in the searched area." *Id*. at 733. To uncover those expectations, Slobogin sought evidence regarding "how society perceives the 'intrusiveness' of government investigative methods." *Id*. According to Slobogin, using the single word "intrusiveness" is less cumbersome than speaking about the impact of government conduct on reasonable expectations of privacy . . . . At the same time, "intrusiveness" captures the core of the construct we sought to investigate . . . ." *Id*.

224. As Slobogin and Schumacher reported, four groups of subjects were recruited on a voluntary basis to complete the first survey instrument, including (1) undergraduate students just beginning a University of Southern California course in law and society (n = 79); (2) University of Florida law students who had not yet taken a course in criminal procedure (n = 52); (3) citizens from the general community in Gainesville, Florida (n = 25); and (4) Australian law students from Monash University, in Melbourne (n = 61). The sample consisted of approximately half males and half females, primarily of the Caucasian race (with a larger number of Hispanics, Latinos, and Asians in the USC sample). It ranged in age from eighteen to seventy (average age = twenty-four), with an average education at the sophomore college level. *Id*. at 737.

225. *Id*. at 736.

226. *Id*.

227. *Id*. at 733-34.

228. Florida v. Riley, 488 U.S. 445, 449 (1989) (upholding as not a "search" police observation of the interior of a partially covered greenhouse in Riley's backyard while circling 400 feet above the greenhouse in a police helicopter).

229. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281 (1983) ("The governmental surveillance conducted . . . in this case amounted principally to the following of an automobile on public streets and highways . . . . [However], [a] person travelling in an automobile on public

three forms of investigation, all of which the Court has exempted from Fourth Amendment scrutiny,[231] were perceived to be significantly more intrusive than the average intrusiveness ratings for activities that are subject to the Fourth Amendment, including a health and safety inspection of a factory (M = 14), and an inspection of a coal mine (M = 25).[232]

As Slobogin and Schumacher demonstrated, judicial conclusions about expectations of privacy do not always correlate with actual expectations of privacy among society.[233] My survey seeks to determine whether the same flaw exists in the *Smith* Court's assumption of risk rationale and content/addressing information distinction, and whether the majority of lower court GPS-tracking cases decided prior to *Jones* were indeed incorrectly decided.

IV. SURVEY DESCRIPTION AND RESULTS

A. Research Design and Hypotheses

In *Jones*,[234] Justice Sotomayor expressed a willingness "to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties,"[235] and specifically doubted that *today's society* would accept the warrantless disclosure of a list of every Web site they had visited, a list of the e-mail addresses with which they have corresponded, and a list of the phone numbers they have dialed or texted.[236]

To test Justice Sotomayor's hypothesis, and to help inform future cases involving electronic monitoring of a suspect's movements in the absence of a physical trespass, an issue potentially resolved under the *Smith* assumption of risk rationale, I designed and administered an original

---

thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

230. California v. Greenwood, 486 U.S. 35 (1988) (ruling that a person does not have a reasonable expectation of privacy in garbage left outside the curtilage of a home for trash removal).

231. *See supra* notes 228-230.

232. SLOBOGIN, *supra* note 15, at 110-11. As Slobogin and Schumacher reported, the least intrusive search and seizure scenario was a search of foliage in a park (M = 6.48), and the most intrusive was a body cavity search at the international border (M = 90.14). Slobogin & Schumacher, *supra* note 221, at 737. Other notable results include an intrusiveness rating of 54.46 for the use of a beeper to track a vehicle, a rating nearly identical to the ratings received for pat-downs (M = 54.76), dog sniffs of one's body (M = 58.33), and the search of cornfields surrounded by a fence and 'No Trespassing' signs (M = 56.58). *See id.* at 737-38.

233. *Id.* at 733-34.

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

235. *Id.* at 957.

236. *Id*.

empirical study which seeks to uncover the actual views of society on these issues.

My survey is similar to the Slobogin and Schumacher surveys, but contains key differences.[237] Most significantly, unlike Slobogin's surveys, in which survey participants were instructed to numerically assess the extent to which they considered each method "an invasion of privacy or autonomy,"[238] my survey simply asks respondents to indicate whether they believe "police should have to [obtain] a search warrant, issued by a judge, before undertaking" each type of activity identified by the survey instrument. Thus, my survey employs a simple "yes" or "no" option, rather than a 100-point scale of invasiveness.[239] This binary method mirrors the analysis required by *Katz*, which effectively requires a reviewing court to determine whether society does, or does not, expect privacy in the particular case at hand.

To test the *Smith* Court's assumption of risk rationale and content/addressing information distinction, my survey poses a series of questions relating to particular forms of communication with different questions for warrantless police access to contents as opposed to addressing information. By comparing the results of these questions within a particular form of communication (e.g., e-mail), my survey enables one to determine whether society indeed distinguishes between content and addressing information.

To test the validity of the pre-*Jones* GPS tracking cases, my survey seeks to determine whether society would expect police to obtain warrants in order to track a vehicle by GPS. While my survey poses a series of questions relating to different types of suspects, this article focuses on just two of those scenarios: one which utilizes the Slobogin approach of assuming an innocent suspect,[240] and one which varies that approach by assuming a suspected drug dealer, the type of suspect that approximates the issue presented in *Jones*.[241] As in *Jones*, my survey assumes GPS tracking accomplished by physical trespass.[242]

---

237. Among other differences, my survey examines particular "search" issues not examined by Slobogin and Schumacher. For example, my survey includes questions relating to police access of computer files and records, including the issues presented in *Forrester*, ones not included in Slobogin's surveys.

238. Slobogin & Schumacher, *supra* note 221, at 735-36.

239. Note, however, that the GPS tracking questions contain three overall options as to whether GPS tracking should be allowed in the absence of a warrant: (1) "Yes, indefinitely," (2) "No," and (3) "Yes, but only for a limited time." If a respondent selects choice (3), he or she is then presented with an additional question asking her to specify the acceptable length of warrantless tracking.

240. *See* Slobogin & Schumacher, *supra* note 221, at 731-32 (explaining the basis for this assumption).

241. The GPS tracking portion of my survey included questions asking respondents to assume (1) a person not convicted of a previous crime and who is currently not suspected of a crime; (2) a person not convicted of a previous crime but who is suspected of having committed a crime; (3) a

Before designing my survey, I developed the various hypotheses set forth below. I then consulted an expert in research design, Dr. Raoul Arreola,[243] who ensured the survey instrument was statistically sound.[244]

The remainder of this section sets forth my various hypotheses. Hypotheses 1 through 7 implicate the *Smith* Court's distinction between content and addressing information, while Hypothesis 8 addresses its assumption of risk rationale. Hypotheses 9 and 10 deal with the GPS tracking method of surveillance. For clarity, I have simplified Hypotheses 1 through 7 by using the same lead-in language contained below.

Hypotheses 1 through 7: A majority of those surveyed believe police should have to obtain a search warrant, issued by a judge after a finding of probable cause, in order to:

> **Hypothesis 1:** Obtain from a third-party internet service provider the names of all website addresses a suspect has visited.
>
> **Hypothesis 2:** Obtain from a third-party provider the e-mail addresses of all individuals a suspect has corresponded with via e-mail.
>
> **Hypothesis 3:** Read the content of their e-mails.
>
> **Hypothesis 4:** Read the content of their text messages.
>
> **Hypothesis 5:** Obtain a list of all phone numbers that have been dialed on one's home phone.

---

person who is a convicted felon and who is not suspected of committing another crime; (4) a person who is a convicted felon but who is currently suspected of committing another crime; (5) a person who has not been convicted of a previous crime but who is a suspected terrorist; (6) a person who has not been convicted of a previous crime but who is a suspected drug dealer; and (7) a person who has not been convicted of a previous crime but who is suspected serial killer. The complete results relating to all seven scenarios will be reported in a future publication.

242. The prefatory language for each of my GPS tracking survey questions clearly anticipates trespassory attachment of the device: "As part of their law enforcement activities the police have attached a GPS (Global Positioning System) device to a person's car without that person's knowledge. They monitor the person's movements for a period of time and then stop."

243. Raoul A. Arreola retired from the University of Tennessee Health Science Center in 2009 with the rank of professor emeritus. He holds a doctorate in educational psychology, specializing in research design, measurement, and evaluation, as well as an undergraduate degree in mathematics and physical sciences. Over the last forty-two years he has worked primarily in the areas of instructional evaluation and development, faculty evaluation and development, and the use of technology in the teaching and learning process.

244. As part of this process, once the survey was complete, I administered the initial draft survey to approximately forty participants, who provided feedback on (1) whether the survey, as a whole, is easily understandable; (2) whether any particular question is unclear or ambiguous; and (3) overall, how easy it was to complete the survey. This process was completed by the end of October 2011.

Hypothesis 6: Obtain a list of all phone numbers that have been dialed on one's cell phone.

Hypothesis 7: Surreptitiously listen in on their phone conversations.

Hypothesis 8 (*Smith*'s Assumption of Risk Rationale): A majority of those surveyed do not agree that when a person gives private information to a bank, a phone company, or any other third-party organization, the police should be able to obtain it without a warrant.

Hypothesis 9: A majority of those surveyed believe police should have to obtain a warrant before police would be permitted to attach a GPS tracking device to the vehicle of an innocent suspect[245] and monitor that vehicle's movements in public.

Hypothesis 10: A majority of those surveyed believe police should have to obtain a warrant before police would be permitted to attach a GPS tracking device to the vehicle of a suspected drug dealer and monitor that vehicle's movements in public.

B. Survey Results

This section separates the results of my survey into two categories: (1) those relating to the *Smith* Court's distinction between content and addressing information along with those relating to its assumption of risk rationale (Hypotheses 1–8); and (2) those relating to GPS tracking accomplished by means of a physical trespass (Hypotheses 9–10).

1. Smith *and* Forrester *Issues*

In *Smith*, the Court ruled that a defendant who makes calls from his home phone assumes the risk that the numbers he conveys to the third party phone company would later be turned over to the police in the absence of a warrant.[246] The Court based this rationale on the idea that callers once had to give a human operator the "addressing information" associated with a phone call; thus, it would be unreasonable to expect privacy in that

245. Survey participants were instructed that an "innocent suspect" refers to an individual who has not previously been convicted of a crime and who is not currently suspected of committing any crime.

246. *See* Smith v. Maryland, 442 U.S. 735, 744, 749 (1979) ("Individuals who [voluntarily] convey information to third parties [i.e., numbers dialed, but not contents of the conversation] have 'assumed the risk' of disclosure to the government." "When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner *assumed the risk* that the company would reveal *to police* the numbers he dialed.") (emphasis added).

information.[247] The content of one's conversations, however, generally remain entitled to Fourth Amendment protection, as established in *Katz*.[248] Through analogies to *Smith*, the content/addressing information distinction currently controls many cutting-edge Fourth Amendment issues, such as those resolved in *Forrester*. In addition, *Smith*'s assumption of risk rationale will likely inform future cases of electronic tracking in the absence of a physical trespass, an issue left unresolved in *Jones*. Thus, the issue is ripe for empirical examination.

Hypotheses 1–7 test, in various ways, the purported distinction between the content of communications and addressing information associated with those communications.[249] Appendix A arranges the results that follow in table form.

Hypotheses 1 and 2 implicate the very issues decided in the Government's favor in *Forrester*, and sought to determine whether the holding of that case is empirically correct. These results are most useful when considered along with the results for Hypothesis 3, which examine expectations of privacy in the content of e-mail communications.

Hypothesis 1 was confirmed. Approximately 63% of survey respondents, or 137 of the 216 individuals completing this question, believed police should have to obtain a warrant before police may obtain from a third-party internet service provider the names of all website addresses a suspect has visited.

Hypothesis 2 was confirmed. Approximately 74% of survey respondents, or 160 of the 216 individuals completing this question, believed police should have to obtain a warrant before police may obtain the e-mail addresses of all individuals a person has corresponded with via e-mail.

---

247. According to *Smith*, the analysis does not change simply because switching equipment has replaced the human operator. *See id.* at 744-45 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.").

248. *See* Katz v. United States, 389 U.S. 347, 352 (1967) ("One who occupies [a public telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

249. *See Smith*, 442 U.S. at 743 ("Although petitioner's conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.").

Hypothesis 3 was confirmed. Approximately 92% of survey respondents, or 198 of the 216 individuals completing this question, believed police should have to obtain a warrant before police may read the content of their e-mails.

Collectively, the results on Hypotheses 1–3 demonstrate that society does, in fact, expect privacy in all aspects of e-mail communications, including both addressing information and content. The same holds true for the IP addresses of internet sites visited.

These results are significant for two reasons. First, these results contradict the rulings of most courts that have considered whether e-mail users may reasonably expect privacy in the content of their e-mail messages.[250] More broadly, these results indicate that society today does not distinguish between the content of a particular form of communication and the addressing information associated with that communication in the sense that society expects privacy in both sets of information.[251]

Hypothesis 5 sought to verify whether the holding of *Smith* is consistent with today's expectations of privacy.[252] Hypothesis 5 was confirmed. On this issue, approximately 73% of survey respondents, or 157 of the 216 individuals completing this question, believed police should have to obtain a warrant before police may obtain a list of all phone numbers a person has dialed on his home phone. These results reveal that *Smith* itself should be revisited because society today does expect privacy in the

---

250. *See* Ray, supra note 197, at 207 (reporting that courts are split as to whether e-mail users can reasonably expect privacy in the contents of their e-mails, but that most courts have found that e-mail users have either a limited or nonexistent expectation of privacy in the content of their messages).

251. There are multiple, possible explanations for society's failure to acknowledge the Court's content/addressing information distinction. In the digital world, content and addressing information data is not so obviously separated in the way it is with earlier forms of communication. For example, with regular postal mail the addressing information is clearly contained on the outside of an envelope, whereas the actual communication is sealed inside. This obvious physical separation naturally creates differing expectations of privacy in the two pieces of information among the general public. However, no clear separation exists in e-mail communications, at least not at the level where most e-mail users interact. For the ordinary member of society, it would be natural to conclude that with e-mail communications, either no aspect of the e-mail communication is protected or all of it is. And, while it is true that a packet of e-mail information "may yield either [addressing] information for the email (the email header), or content information (the email itself), or both (in the case of a short email that can fit the entire header and message on one packet)," the ordinary member of society would presumably not be aware of these technological concepts in the way they are with ordinary postal mail. *See generally* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 614-15 (2003) (discussing the analogy between posted mail and e-mail).

252. *See Smith*, 442 U.S. at 745-46 (holding that "[t]he installation and use of [a] pen register [a device that records numbers dialed from a home telephone] . . . was not a 'search,' and no warrant was required").

addressing information associated with their telephone communications, a result contrary to the explicit holding of *Smith*.

Hypothesis 6 applied the *Smith* issue to cell phones. Hypothesis 6 was confirmed. Once again, a majority of those surveyed—approximately 72%—believed police should have to obtain a warrant before police may obtain a list of all phone numbers that have been dialed from one's cell phone. Thus, survey respondents did not distinguish between home phones and cell phones.

Hypotheses 4 and 7 were content-related hypotheses involving text messages and phone conversations. Each of these hypotheses was confirmed.

Regarding Hypothesis 4, approximately 92% of those surveyed, or 197 of the 215 individuals completing this question, believed police should have to obtain a warrant before police may read the content of their text messages.

Regarding Hypothesis 7, approximately 95% of those surveyed, or 206 of the 216 individuals completing this question, believed police should have to obtain a warrant before police may surreptitiously listen in on their phone conversations. These results should not be surprising given society's general familiarity with the legal restrictions upon wiretapping.[253]

Hypothesis 8 tested the assumption of risk rationale underlying *Smith*, and sought to determine whether society disagrees with that rationale.

Hypothesis 8 was confirmed. Contrary to *Smith*, society does not believe that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and therefore "assumes the risk" of disclosure to the government.[254] Of the 216 individuals completing this question, 186 of the survey respondents—or 86.1%—believed police should have to obtain a warrant before accessing private information conveyed to a bank, a phone company, or any other third-party organization. As Justice Sotomayor speculated in *Jones*,[255] the assumptions underlying *Smith* are no longer valid.[256]

---

253. Since 1968, this issue has been governed by the Omnibus Crime and Control and Safe Streets (Wiretap) Act of 1968, which was amended by the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, and is now codified in various sections of Title 18 of the United States Code.

254. *See Smith*, 442 U.S. at 743-44 (citing *United States v. Miller*, 425 U.S. 435, 442–444 (1976) (holding that a bank depositor has no "legitimate 'expectation of privacy'" in financial information "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business")).

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

256. While this article does not attempt to explain the basis for these results, I will tentatively note that there are multiple, possible explanations for society's disagreement with the content/addressing information distinction. In the digital world, both content and addressing information are bundled

2. GPS Tracking Issues

Hypotheses 9 and 10 dealt with the GPS tracking cases. The goal in this portion of the survey was to empirically determine society's views regarding warrantless GPS tracking accomplished by means of a physical trespass. While my survey poses a series of questions relating to different types of suspects, this article focuses on just two of those scenarios: one which utilizes the Slobogin approach of assuming an innocent suspect,[257] and one which varies that approach by assuming a suspected drug dealer, the issue that most closely approximates the issue in *Jones*.[258]

Hypothesis 9 posited that a majority of those surveyed believe police should have to obtain a search warrant, issued by a judge after a finding of probable cause, before police would be permitted to attach a GPS tracking device to the vehicle of an innocent suspect and monitor that vehicle's movements in public. As used here, an "innocent suspect" refers to an individual who has not previously been convicted of a crime and who is not currently suspected of committing any crime.

Hypothesis 9 was confirmed. Approximately 89% of respondents who answered this question, or 205 of the 230 individuals, believed police should have to obtain a warrant before police could lawfully attach a GPS tracking device to the vehicle of an innocent suspect and monitor that vehicle's movements.

Hypothesis 10 posited that a majority of those surveyed believe police should have to obtain a search warrant before police would be permitted to attach a GPS tracking device to the vehicle of a suspected drug dealer and monitor that vehicle's movements in public, an issue that approximates the issue in *Jones*.

Hypothesis 10 was confirmed. On this issue, a majority of respondents, approximately 53%, or 118 of the 223 respondents who

---

together in one package. Forensics analysts have to splice the data. Thus, content and addressing information data is not so clearly separated in the way it is with earlier forms of communication. For example, with regular postal mail the addressing information is contained on the outside of the envelope, whereas the actual communication is sealed inside. This physical separation naturally leads to differing expectations of privacy in the two pieces of information. However, no clear separation exists in e-mail communications. With e-mail communications, either no aspect of the e-mail communication is protected, or all of it is.

257. *See* Slobogin & Schumacher, *supra* note 221, at 731-32 (explaining the basis for this assumption).

258. The GPS tracking portion of my survey included questions asking respondents to assume (1) a person not convicted of a previous crime and who is currently not suspected of a crime; (2) a person not convicted of a previous crime but who is suspected of having committed a crime; (3) a person who is a convicted felon and who is not suspected of committing another crime; (4) a person who is a convicted felon but who is currently suspected of committing another crime; (5) a person who has not been convicted of a previous crime but who is a suspected terrorist; (6) a person who has not been convicted of a previous crime but who is a suspected drug dealer; and (7) a person who has not been convicted of a previous crime but who is suspected serial killer. The complete results relating to all seven scenarios will be reported in a future publication.

answered this question, believed police should have to obtain a warrant before they would be permitted to track an individual by GPS for *any period of time*. Only 46 of the 223 respondents, or approximately 21%, would permit warrantless GPS tracking to extend 21 days or longer. Of the remaining 59 respondents, 51 would not have permitted such tracking to extend beyond ten days in the absence of a warrant.

Given that only 1 in 5 respondents would permit warrantless GPS tracking to extend 21 days or longer, the Government's analogy to visual observation of a vehicle in public, as argued in *Jones*[259] (a case involving a 28-day warrantless GPS tracking) simply fails to adequately resolve the issue. Indeed, under the Government's argument in *Jones*, warrantless GPS tracking would be permitted to continue indefinitely without ever triggering the requirement of a warrant. However, only 24.2% of survey respondents would have been willing to permit warrantless GPS tracking to extend beyond 10 days. This is strong evidence that the unanimous *Jones* decision represents an accurate reflection of society's privacy expectations on this issue.

V. THE FUTURE OF CELL PHONE TRACKING

This section addresses the impact of my survey results on the warrantless monitoring of a suspect's movements by cell phone data in the absence of a physical trespass, the investigative method most likely to be utilized in the wake of *Jones*.

In striking down the warrantless attachment and subsequent use of a GPS tracking device in *Jones*, the majority based its decision on the physical trespass that was required to monitor the vehicle's movements in that case.[260] *Jones* did not address whether police may obtain similar tracking information directly from a cell phone provider.

Given the narrow *Jones* holding, the concurring Justices in *Jones* worried that "the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones."[261] This next generation of

---

259. In its *Jones* brief, the United States argued that individuals have no reasonable expectation of privacy in information knowingly exposed to public view, which directly applied to Jones. *See* Petitioner's Brief on the Merits at 18, 38, United States v. Jones, No. 10-1259, 2012 WL 171117 (2012), 2011 WL 5094951.

260. According to the majority, "the Government's *installation* of a GPS device on a target's vehicle, *and its use* of that device to monitor the vehicle's movements, constitutes a 'search.'" United States v. Jones, 132 S.Ct. 945, 949 (2012) (emphasis added). Crucial to the majority's analysis is the fact that "Jones . . . possessed the Jeep at the time the Government trespassorily inserted the [GPS] device." *Id*. at 952.

261. *Jones*, 132 S.Ct. at 954 (Sotomayor, J., concurring). *See also* People v. Weaver, 12 N.Y.3d 433, 442 (2009) ("[W]ith GPS becoming an increasingly routine feature in cars and cell phones, it will

GPS tracking could be analyzed in one of two ways. On the one hand, obtaining tracking information directly from a third-party provider is presumably controlled by *Smith*'s assumption of risk rationale, which would exempt this information from Fourth Amendment protection. On the other hand, factory-installed GPS devices, whether contained in vehicles or smartphones, enable the Government to obtain roughly the same location information provided by the GPS device utilized in *Jones*. With very little difference between the types of information made available by both devices, this raises the possibility of being struck down under the logic of the *Jones* concurrence, which emphasized length of surveillance as a critical factor.[262]

Beyond GPS, other similar types of searches are currently being employed by law enforcement. Cell phone location data, for example, is often used to reveal where a cell phone was located at a particular point in time by identifying which cell tower communicated with the cell phone while the phone was either turned on or utilized to make a call.[263] In urban areas, where cell towers are often only hundreds of feet apart, cell location data makes it possible to determine a person's movements with precision.[264] Indeed, a suspect's "exact location" can be determined through methods of triangulation from various cell towers.[265] Cell phone companies maintain records of this switching information,[266] making it possible for the Government to request either "real time" cell site information or historical cell site information.[267] The tracking of a cell

be possible to tell from the technology with ever increasing precision who we are and are not with, when we are and are not with them, and what we do and do not carry on our persons—to mention just a few of the highly feasible empirical configurations.").

262. *See supra* notes 85-89 and accompanying text. As the *Jones* majority noted, the inside/outside distinction between *Knotts* and *Karo* is also potentially relevant here. *See supra* notes 53-61 and accompanying text.

263. United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *1 (N.D. Ind. Mar. 26, 2010).

264. *In re* Application of the United States, 405 F.Supp.2d 435, 449 (S.D.N.Y. 2005).

265. United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *10 (N.D. Ga. April 21, 2008). *See also In re* Application of the United States, 509 F. Supp. 2d 76, 78 (D. Mass. 2007) ("cell site information coupled with a basic knowledge of trigonometry makes it possible to identify with reasonable certainty the location from which a call was made").

266. *See In re* Application of the United States, 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011) ("If a user's cell phone has communicated with a particular cell-site, this strongly suggests that the user has physically been within the particular cell-site's geographical range. By technical and practical necessity, cell-phone service providers keep historical records of which cell-sites each of their users' cell phones have communicated. The implication of these facts is that cellular service providers have records of the geographic location of almost every American at almost every time of day and night.").

267. *See In re Application of the United States*, 405 F.Supp.2d at 437 ("As a cell phone user moves from place to place, the cell phone automatically switches to the tower that provides the best reception," which in turn enables the Government to obtain "cell-site information concerning the physical location of the antenna towers associated with the beginning and termination of calls to and from a particular cellphone."). *See also id.* at 449 (noting the distinction between requests for "historical versus real time data").

phone in this manner does not require the installation of any device; rather, the telephone itself does the work,[268] making the *Jones* majority's trespass rationale inapplicable.

In light of the expanding use of cellular network information by law enforcement, courts have begun to grapple with the Fourth Amendment implications of cell phone tracking. Several courts, in particular, have addressed *Katz*-based objections to acquiring cell location data in the absence of a warrant, and their opinions confirm the ease in which *Smith*'s assumption of risk rationale can be extended to validate this next generation of warrantless suspect monitoring.[269]

United States v. Graham,[270] decided just a few weeks after *Jones*, illustrates the typical method of analysis employed by courts that have upheld the warrantless gathering of cell location data. In *Graham*, the United States District Court for the District of Maryland ruled that the government does not need probable cause or a warrant to force a cell phone provider to disclose more than seven months of data on the movements of one of its customers.[271] In that case, two defendants were thought to have conducted a series of armed robberies, and a key piece of evidence linking them to each robbery was data about the movements of their cell phones.[272]

---

268. *In re Application of the United States*, 509 F. Supp. 2d at 81 n.11.

269. *See, e.g., Suarez-Blanca*, 2008 WL 4200156, at *8-11 (applying the *Smith* and *Miller* assumption of risk rationale and concluding that the government's warrantless acquisition of two months of historical cell site information for various phones linked to defendants did not violate the Fourth Amendment); United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010) (agreeing with "the well-reasoned decision of the *Suarez-Blanca* court that the logic of the Supreme Court in *Smith* and *Miller* should be extended to cell-site data"); United States v. Dye, No. 1:10CR221, 2011 WL 1595255, at *9 (N.D. Ohio Apr. 27, 2011) (citing *Smith* for the proposition that "there is no reasonable expectation of privacy in cell phone records," and finding, without discussion, no reasonable expectation of privacy in "cell site location information"); United States v. Velasquez, No. CR 08-0730 WHA, 2010 WL 4286276, at *4-*5 (N.D. Cal. Oct. 22, 2010) (noting a potential application of *Smith v. Maryland* and rejecting the defendant's Fourth Amendment challenge to cell site location information, reasoning that cell site location information "could have been obtained through physical observation of defendant," that cell site location information "is less accurate than information obtained by GPS tracking technology;" that "cell phones are voluntarily carried by their users and may be turned on or off at will;" and that "the only information obtained here was retrospective in nature," rather than real-time or prospective). *See also In re Application of the United States*, 509 F. Supp. 2d at 80-82 (granting the government's application for an order directing cellular telephone companies to disclose historical cell site information and stating, "[t]he location of a cell tower in relation to the point of origin (or termination) of a call discloses nothing about the substance of the call itself. It is therefore 'noncontent' information.").

270. United States v. Graham, No. RDB-11-0094, 2012 WL 691531 (D. Md. March 1, 2012).

271. *Id*. at *5.

272. On March 25, 2011, the government applied for an order from a Magistrate Judge pursuant to the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq*., which ordered Sprint/Nextel, Inc. to disclose to the government the identification and address of cellular towers (cell site locations) related to the use of the defendants' cellular telephones. *Id*. at *1. The government sought cell site location data for the periods of August 10-15, 2010; September 18-20, 2010; January 21-23,

The defendants sought to suppress this evidence because the government did not get a warrant before seeking the data.[273] Invoking *Smith*, the government argued that the defendants have no Fourth Amendment expectation of privacy in business records voluntarily conveyed to a third party.[274] According to the government, the voluntary disclosure of cell site location data is analogous to dialed telephone numbers captured by pen registers and bank records disclosed to banks, which are exempt from Fourth Amendment protection.[275]

The *Graham* court agreed with the government, ruling that "the [d]efendants in this case do not have a legitimate expectation of privacy in the historical cell site location records acquired by the government."[276] According to the court, "[l]ike the dialed telephone numbers in *Smith*, the [d]efendants in this case voluntarily transmitted signals to cellular towers in order for their calls to be connected,"[277] and "[t]he cellular provider then created internal records of that data for its own business purposes."[278]

In reaching this result, the *Graham* court described *Jones* as "relevant but not controlling in this case."[279] The *Graham* court distinguished GPS tracking on the grounds that historical cell site location data exposes only historical evidence of a suspect's past locations,[280] whereas GPS technology reveals the location and movements of a suspect in real time,

---

2011; and February 4-5, 2011. *Id.* In its application, the government alleged that the information sought was relevant to an ongoing investigation of robberies the defendants were suspected of committing. *Id*. By identifying the location of cellular towers accessed by the defendants' phones during the relevant time periods, the government sought to more conclusively link the defendants with the prior robberies. *Id*. The magistrate judge issued the order under the reasonable suspicion standard utilized by the Stored Communications Act. *Id.* at *2. In a second order, the Government sought cell site location data for the periods July 1, 2010 through February 6, 2011. *Id*. This order was granted by a separate magistrate judge under the same reasonable suspicion standard. *Id*. The government's request resulted in the release of almost 22,000 individual cell site location data points. *Id*.

273. *Id*. The *Graham* defendants did not argue that the Stored Communications Act is unconstitutional on its face, but instead argued that the length of time and extent of the cellular phone monitoring conducted in their particular case intruded on their expectation of privacy and was therefore unconstitutional. *Id*.

274. *Id*. at *3.

275. *Id*.

276. *Id*. at *5.

277. *Id*. at *13.

278. *Id*. *See also id*. at *14 ("Like the bank records at issue in *Miller*, [and] the telephone numbers dialed in *Smith* . . . , historical cell site location records are records created and kept by third parties that are voluntarily conveyed to those third parties by their customers. As part of the ordinary course of business, cellular phone companies collect information that identifies the cellular towers through which a person's calls are routed.").

279. *Id*. at *20 n.2.

280. While this may be a plausible distinction of *Jones*, the distinction would not apply in those instances in which the government seeks "real time" cell site information. *See In re* Application of the United States, 405 F.Supp.2d 435, 449 (S.D.N.Y. 2005) (noting the distinction between requests for "historical versus real time data").

and is "far more precise than the historical cell site location data at issue here."[281]

Like *Graham*, a majority of courts to have considered the issue have invoked *Smith*'s assumption of risk rationale and concluded that the acquisition of historical cell site location data does not implicate the Fourth Amendment, regardless of the time period involved.[282] However, not all courts have chosen to follow the approach of *Graham*, especially for lengthier periods of surveillance. For example, the Eastern District of New York and the Southern District of Texas have concluded that applications seeking cell site location data may be granted only after a showing of probable cause, rejecting the more lenient standard of specific and articulable facts employed by the Stored Communications Act.[283]

Extending *Smith*'s assumption of risk rationale to these cases is a flawed approach.[284] First, my survey demonstrates that the average citizen would not expect the government to obtain this type of information from a third-party provider in the absence of Fourth Amendment protection. Indeed, 86.1% of my survey respondents disagreed with the proposition that whenever a defendant exposes his otherwise private information to a third party, such as a cell phone company, the defendant has knowingly exposed that same information to law enforcement.

Moreover, the rationale underlying *Smith*, even if empirically sound, does not account for many of the factors that would control this unique issue. For example, if length of surveillance is a potentially controlling factor, as the five concurring Justices in *Jones* speculated and as courts

---

281. *Graham*, 2012 WL 691531, at *6.

282. *See, e.g.*, United States v. Dye, No. 1:10CR221, 2011 WL 1595255, at *9 (N.D. Ohio Apr. 27, 2011); United States v. Velasquez, No. CR 08-0730 WHA, 2010 WL 4286276, at *5 (N.D. Cal. Oct. 22, 2010); United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *8-11 (N.D. Ga. Apr. 21, 2008); *In re* Application of the United States, 509 F. Supp. 2d 76, 80-81 (D. Mass. 2007).

283. *See In re* Application of the United States, 809 F.Supp.2d 113 (E.D.N.Y. 2011); *In re* Application of the United States, 747 F.Supp.2d 827 (S.D. Tex. 2010) (Smith, Mag. J.), *appeal docketed*, No. 11-20554 (5th Cir. Dec. 14, 2011); *In re* Application of the United States, 736 F. Supp. 2d 578 (E.D.N.Y. 2010) (Orenstein, Mag. J.), *rev'd* No. 10-MC-0550 (E.D.N.Y. Nov. 29, 2011) (unpublished order noting written opinion to follow).

284. Some courts agree. *See, e.g.*, *In re* Application of the United States, 747 F.Supp.2d 827, 844 (S.D.Tex. 2010) ("Unlike the bank records in *Miller* or the phone numbers dialed in *Smith*, cell site data is neither tangible nor visible to a cell phone user. When a user turns on the phone and makes a call, she is not required to enter her own zip code, area code, or other location identifier. None of the digits pressed reveal her own location. Cell site data is generated automatically by the network, conveyed to the provider not by human hands, but by invisible radio signal. Thus, unlike in *Miller* or *Smith*, where the information at issue was unquestionably conveyed by the defendant to a third party, a cell phone user may well have no reason to suspect that her location was exposed to anyone. The assumption of risk theory espoused by *Miller* or *Smith* necessarily entails a knowing or voluntary act of disclosure," which does not apply here.).

addressing cell site location issues have found,[285] then analogy to *Smith*, which entirely disregards that variable, is too simplistic. Also, it is not entirely clear that cell phone users "voluntarily convey" the locations of their phones to their providers, or somehow make a knowing choice to share evidence of their criminal activities with another, simply by using their phones.[286] Given the widespread use of cell phones, the possibility of using cell site location data to obtain detailed location information on both criminal suspects and law-abiding citizens is also significant.[287]

In sum, courts in these cases are faced with two options: analogize the case to *Smith* or analyze the case on its merits by considering the actual expectations of privacy society ascribes to this particular form of investigation. As my survey demonstrates, the assumption of risk rationale underlying *Smith* does not comport with society's actual expectations of privacy. Thus, analogy to *Smith* is a flawed approach. Without the benefit of analogy, courts should be careful to assess society's actual expectations of privacy in the particular form of surveillance at hand, and empirical evidence represents the best measure of those expectations.

VI. CONCLUSION

The gap between traditional forms of police surveillance and technologically enhanced methods of surveillance is vast and continues to grow at a rapid pace.[288] Whether the Fourth Amendment should interpose

---

285. *See, e.g.*, *In re* Application of the United States, 809 F. Supp. 2d 113, 118-19 (E.D.N.Y. 2011) ("Here, the Government has requested . . . at least 113 days of constant surveillance of an individual . . . . [T]he application seeks information that is protected by the Fourth Amendment . . . . The cell-site-location records sought here captures enough of the user's location information for a long enough time period—significantly longer than the four weeks in *Maynard*—to depict a sufficiently detailed and intimate picture of his movements to trigger the same constitutional concerns as the GPS data in *Maynard*.").

286. *In re* Application of the United States, 620 F.3d 304, 317-18 (3d Cir. 2010) ("[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way . . . [because] it is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information. Therefore, when a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all.").

287. *See In re* Application of the United States, 809 F.Supp.2d 113, 119-20 (E.D.N.Y. 2011) ("[T]he collection of cell-site-location records effectively enables 'mass' or 'wholesale' electronic surveillance, and raises greater Fourth Amendment concerns than a single electronically surveilled car trip. This further supports the court's conclusion that cell-phone users maintain a reasonable expectation of privacy in long-term cell-site-location records and that the Government's obtaining these records constitutes a Fourth Amendment search.").

288. *See generally* SLOBOGIN, *supra* note 15.

the judiciary on such surveillance poses "momentous issues."[289] Forms of surveillance only recently made possible include mass surveillance by way of cameras installed around major cities, some of which are equipped with wide angle lenses, night vision, zoom, and recording capabilities;[290] handheld devices that produce silhouettes of objects concealed by clothing or cars, including some that even reveal anatomical details;[291] and handheld devices that covertly retrieve much of a cell phone's contents from up to 150 feet away.[292]

When determining whether to impose constitutional restrictions on such forms of surveillance, courts often fall back on the rules and rationales from an earlier technological era. Yet the rulings associated with more traditional forms of surveillance do not always comport with society's actual expectations of privacy and often fail to account for relevant differences between the analogized cases. By utilizing the empirical approach, courts will reach more sensible results in such cases, ones that comport with society's actual expectations of privacy in the particular form of surveillance at hand.

Because of the very nature of the *Katz* test, which by its very wording hinges upon society's actual expectations of privacy, the empirical approach is particularly well-suited to resolve Fourth Amendment "search" questions. Yet, so often in these cases, courts resort to easy analogies and fail to consider actual expectations of privacy. The potential flaws of analogical reasoning are particularly apparent in the GPS tracking cases decided prior to *Jones*, and in cases involving police access of certain electronic files. As this article has demonstrated, society today is not willing to accept GPS tracking in the absence of a warrant, particularly with respect to the type of suspect at issue in *Jones*. Whether that result would apply to other types of suspected offenses, and whether that result would apply in the absence of a physical trespass, are issues that deserve careful analysis.

---

289. United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

290. *See* SLOBOGIN, *supra* note 15, at 81-84 (describing the prevalence of public surveillance using camera technology, and describing such surveillance as "increasing at an exponential rate").

291. *See id*. at 84.

292. Such devices were allegedly used by Michigan State Police Officers in recent years without the knowledge of Michigan citizens. *See* Steve Tarlow, *Michigan Police Scan Driver Cell Phones During Traffic Stops*, NEWSTYPE (Apr. 20, 2011), http://www.newsytype.com/5614-aclu-michigan-police-phone-scan/ (describing the allegations). The CelleBrite UFED, a mobile forensics device that works with 4,000 cell phone models and can break password protection, can reportedly copy all photos and video from an iPhone in less than 90 seconds. *See* CELLBRITE.COM, http://www.cellebrite.com/mobile-forensics-products/forensics-products/ufed-logical.html (last visited Apr. 11, 2012) (describing the capabilities of the CelleBrite mobile forensics device). *See also* United States v. Flores-Lopez, 670 F.3d 803 (7th Cir. 2012) (describing the technology).

APPENDIX A: *SMITH*-RELATED HYPOTHESES BY FORM OF COMMUNICATION

The table below vertically groups each hypothesis as either a content-based or addressing-related question, then matches particular forms of communication horizontally to highlight the comparison between content and addressing information.

Form of Communication	**Addressing Information Associated with this Form of Communication**	**Content of Communication**
E-mail	74.1% of survey respondents, or 160 of the 216 individuals completing this question, would require a warrant before police may obtain the e-mail addresses of all individuals a person has corresponded with via e-mail.	91.7% of survey respondents, or 198 of the 216 individuals completing this question, would require a warrant before police may read the content of a person's e-mails.
Telephone Conversations (from home phone)	72.7% of survey respondents, or 157 of the 216 individuals completing this question, would require a warrant before police may obtain a list of all phone numbers a person has dialed on his home phone (contradicting *Smith*).	95.4% of survey respondents, or 206 of the 216 individuals completing this question, would require a warrant before police may listen in on a person's conversations without their knowledge.
Telephone Conversations (from cell phone)	71.8% of survey respondents, or 155 of the 216 individuals completing this question, would require a warrant before police may obtain a list of all phone numbers a person has dialed on his cell phone.	95.4% of survey respondents, or 206 of the 216 individuals completing this question, would require a warrant before police may listen in on a person's conversations without their knowledge.

APPENDIX B: DETAILED SURVEY RESULTS

Scenario #1: PERSON NOT ACCUSED & NOT SUSPECTED		
If the person has *NOT BEEN CONVICTED* of a crime and *IS NOT SUSPECTED* of committing any crime, do you feel that the police should be able to track the individual without getting a search warrant?		
	Response Count	Response Percentage
YES – INDEFINITELY	7	3.0%
YES – BUT FOR A LIMITED TIME ONLY	18	7.8%
NO – THEY SHOULD GET A SEARCH WARRANT	205	89.1%
TOTAL N	230	

Scenario #1: *If YES But For A Limited Time Only*		
If you selected "yes, but for a limited time only," how long do you believe that the police should be allowed to track the individual WITHOUT getting a warrant?		
	Response Count	*Response Percentage*
Less than 1 day	4	17.4%
1 Day	3	13.0%
2 Days	1	4.3%
3 – 5 Days	9	39.1%
6 – 10 Days	5	21.7%
11 – 20 Days	0	0.0%
21 Days or Longer	1	4.3%
TOTAL N	23	

Scenario #2: PERSON IS A SUSPECTED DRUG DEALER		
If the person *HAS NOT BEEN CONVICTED* of a crime but *IS A SUSPECTED DRUG DEALER*, do you feel that the police should be able to track the individual without getting a search warrant?		
	Response Count	Response Percentage
YES – INDEFINITELY	32	14.3%
YES – BUT FOR A LIMITED TIME ONLY	73	32.7%
NO – THEY SHOULD GET A SEARCH WARRANT	118	52.9%
TOTAL N	223	

Scenario #2: *If YES But For A Limited Time Only*		
If you selected "yes, but for a limited time only," how long do you believe that the police should be allowed to track the individual WITHOUT getting a warrant?		
	Response Count	*Response Percentage*
Less than 1 day	3	4.1%
1 Day	5	6.8%
2 Days	7	9.6%
3 – 5 Days	16	21.9%
6 – 10 Days	20	27.4%
11 – 20 Days	8	11.0%
21 Days or Longer	14	19.2%
TOTAL N	73	

EMAIL, INTERNET, AND CELL PHONE SEARCHES					
For each of the following please indicate whether you feel the police should have to get a search warrant, issued by a judge, before undertaking the type of search described.					
	YES, Need a search warrant		NO, Do not need a search warrant		Total Response Count
	#	%	#	%	#
Obtaining a list of web sites a person has visited from a third-party internet service provider.	137	**63.4%**	79	**36.6%**	216
Obtaining a list of all email addresses to whom a person has sent email messages and from whom that person has received email messages.	160	**74.1%**	56	**25.9%**	216
Reading the contents of a person's emails.	198	**91.7%**	18	**8.3%**	216
Reading the contents of a person's text messages.	197	**91.6%**	18	**8.4%**	215
Obtaining a list of all the phone numbers that have been dialed on a person's home phone.	157	**72.7%**	59	**27.3%**	216
Obtaining a list of all the phone numbers that have been dialed on a person's cell phone.	155	**71.8%**	61	**28.2%**	216
Listening in on the person's telephone conversations without their knowledge.	206	**95.4%**	10	**4.6%**	216

USING PRIVATE INFORMATION		
Do you feel that when a person gives private information to a bank, a phone company, or any other third-party organization, it means that the information is now 'public' and that the police should be able to obtain it without a warrant?		
	Response Count	*Response Percentage*
YES – Once I give the information out to anyone it is 'public'	30	13.9%
NO – My information stays private	186	86.1%
TOTAL N	216	

DEMOGRAPHIC INFORMATION

17. Are you male or female?		
	Response Count	*Response Percentage*
Male	89	41.2%
Female	127	58.8%
TOTAL N	216	

18. Which category below includes your age?		
	Response Count	*Response Percentage*
17 or younger	0	0.0%
18 - 20	6	3.0%
21 - 29	75	37.5%
30 - 39	47	23.5%
40 - 49	17	8.5%
50 - 59	24	12.0%
60 or older	31	15.5%
TOTAL N	200	

19. Are you a currently enrolled student in a school or college?		
	Response Count	*Response Percentage*
YES	87	40.3%
NO	129	59.7%
TOTAL N	216	

20. (IF YES TO STUDENT ITEM ABOVE): What is your status as a student?		
	Response Count	*Response Percentage*
Full-time	83	95.4%
Part-time	4	4.6%
TOTAL N	87	

21: What is the highest level of school you have completed or the highest degree you have received?		
	Response Count	*Response Percentage*
Less than high school degree	1	0.5%
High school degree or equivalent (e.g., GED)	4	1.9%
Some college but no degree	22	10.2%
Associate Degree	14	6.5%
Bachelor Degree	108	50.0%
Graduate Degree	67	31.0%
TOTAL N	216	

22: Which of the following categories best describes your employment status?		
	Response Count	*Response Percentage*
Employed, working 1 – 39 hours per week	46	21.3%
Employed, working 40 or more hours per week	82	38.0%
Not employed, looking for work	17	7.9%
Not employed, NOT looking for work	48	22.2%
Retired	22	10.2%
Disabled, not able to work	1	0.5%
TOTAL N	216	

23: Are you now married, in a relationship with a domestic partner, widowed, divorced, separated, or single?		
	Response Count	*Response Percentage*
Married	91	42.3%
In a Relationship With a Domestic Partner	19	8.8%
Widowed	2	0.9%
Divorced	10	4.7%
Separated	0	0.0%
Single (never married)	93	43.3%
TOTAL N	215	

24: Are you White, Black or African-American, American Indian or Alaskan Native, Asian, Native Hawaiian or other Pacific islander, or some other race?		
	Response Count	*Response Percentage*
White – Non Latino	157	75.8%
White - Latino	21	10.1%
Black or African-American	11	5.3%
American Indian or Alaska Native	0	0.0%
Asian	10	4.8%
Native Hawaiian or other Pacific Islander	0	0.0%
From multiple races	8	3.9%
TOTAL N	207	