SURVEILLANCE TECHNOLOGY AND THE LOSS OF SOMETHING A LOT LIKE PRIVACY: AN EXAMINATION OF THE "MOSAIC THEORY" AND THE LIMITS OF THE FOURTH AMENDMENT

COURTNEY E. WALSH[1]

1. LL.M., Harvard Law School; J.D, University of Florida. I would like to offer my sincere thanks to Prof. Philip Heymann and Prof. Jerold Israel for their mentorship in the development of this article. Also, I would like to thank several colleagues of mine for their friendship and insights along the way: Siddhartha Velandy, Saptarishi Bandopadhyay, Ricardo Gomez, Marcin Kilanowski, and Christopher Sajdera. And finally, I wish to express my deepest gratitude to my wife, Maggi, for her committed partnership in this and in all of life's worthwhile endeavors.
The views expressed in this article are solely those of the author and in no way represent those of the U.S. Marine Corps, the Department of Defense, or the U.S. Government.

INTRODUCTION: PUBLIC . . . PRIVACY?

In an article in the Kansas Law Review, Chief Justice William Rehnquist offered a now well-known hypothetical that summarized the tension inherent in the normative concept of "privacy" and its particular manifestation in Fourth Amendment jurisprudence.[2] In his hypothetical, Chief Justice Rehnquist asks the reader to imagine a police officer standing in the parking lot of a bar from the hours of 5:30 p.m. to 7:30 p.m. every day.[3] Each day, the police officer takes notes and records the license plates of every vehicle that parks in the lot adjacent to the bar in order to identify the bar's "regulars." At this point, assume that the police officer has no particular reason to know of any unlawful conduct by the bar's patrons.

Rehnquist imagines that this type of persistent surveillance activity, conducted without suspicion of criminal wrongdoing, and done solely for the purpose of recording names for future police reference is police conduct that most persons would rightly, in his appraisal, feel uneasy about, intuiting it to be an inappropriate law enforcement function.[4] Despite the sense that people would find this type of "extreme" surveillance activity disturbing, Chief Justice Rehnquist purposely avoids labeling this disturbed sensibility as "privacy."[5] For him, "there can be no question that driving an automobile down a public street and into a parking lot of a bar, which is itself open to the general public, is not in any normal sense of the word a

2. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 90 (2007); William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come Along Way, Baby*, 23 U. KAN. L. REV. 1, 9 (1974). At the time he wrote these words, Chief Justice Rehnquist was a newly appointed Associate Justice to the United States Supreme Court. Rehnquist, *supra*.

3. Rehnquist, *supra* note 2, at 9.

4. *Id.*

5. *Id.*

'private' act."[6] Instead, as any member of the general public is free to engage in the same observational conduct attributed to the police in this hypothetical, this uneasiness is merely a sense that unwarranted, persistent surveillance is not a proper governmental function.[7] For the Chief Justice, the ability or inability to exclude observation of one's conduct – call it secrecy[8] – is the touchstone of constitutionally cognizable "privacy."

Chief Justice Rehnquist described these facts as "extreme,"[9] which is correct in that it would be unusual in the United States for a law enforcement officer to engage in prolonged visual surveillance simply for the sake of collecting volumes of information on persons not suspected of any wrongdoing. However, in a more modern sense, this hypothetical is no longer so extreme.[10] Replacing the formerly necessary beat-cop with technologically-enhanced surveillance systems makes the execution of persistent government observation in public spaces more covert and less costly.[11] Because of the heightened surveillance capabilities created through technological advancement, the Chief Justice's then-hypothetical problem seems far less hypothetical today. Specifically, in a post-9/11 world, where government agencies have undergone a clear tactical shift from post-crime investigation to a mode of preventative detection, government demand continues to push development in the field of surveillance technologies.[12] This has had the effect of not only making technology more operationally efficient—"better" in a purely abstract sense—but also increasing its supply, decreasing cost, and therefore, broadening the market of users.[13]

As a result, it is not only the most well-funded federal and international law enforcement, military, and intelligence agencies that have access to top-line surveillance technologies, but also state and local law enforcement.[14] The convergence of these and other factors—changed mission demands, improved technologies, increased cost efficiency, and a constrained fiscal environment—substantially shifts many of the assumptions underly-

6. *Id.*

7. *Id.*

8. United States v. Jones, 132 S. Ct. 945, 957 (2011) (Sotomayor, J., concurring) ("[O]ur Fourth Amendment jurisprudence [tends] to treat secrecy as a prerequisite for privacy.").

9. Rehnquist, *supra* note 2, at 9.

10. *See, e.g.*, SLOBOGIN, *supra* note 2, at 90–91.

11. *See id.* (discussing this effect in the specific context of surveillance cameras and explaining that the principle applies as well to a broad spectrum of surveillance modalities).

12. *See* TOM BINGHAM, THE RULE OF LAW 134–35, 155–58 (2010).

13. *See infra* Part IV. A–B.

14. *Id.*

ing the Fourth Amendment's jurisprudence,[15] especially as to the freedoms a person may possess outside of his or home. Where society might have once been able to depend on technology's cost to act as a self-regulating tool, that assumption has since been turned on its head. As market forces no longer exert *de facto* regulatory force over the widespread employment of surveillance technologies, it may now be necessary to assess the need for greater positive control through *de jure* regulatory mechanisms. Assuming that a policy response is necessary in light of these dynamic forces, the question then is what form and through which branch of government should any regulatory action emanate?

In order to answer that question, it is necessary to isolate what "sensibility" or "right" would be lost as a result of enhanced technological surveillance of public space. At its philosophical core, the hypothetical posed by Chief Justice Rehnquist and the not-so-hypothetical modern manifestation of it suggests that there is, at some intuitive level, a normative belief that one should be free from persistent visual observation—even when in public. However, despite the predictable unease that would be felt by any person being observed in public, the Fourth Amendment—even as the Constitution's "core" privacy right,[16] would almost as predictably, not prevent the government from engaging in such surveillance practices—as the constitutionally assigned plain meaning of "privacy" excludes that "which is itself open to the general public."[17] The source of the tension, then, is that the social norm proposed by the Chief Justice—that persons, even though present in public space, should not be subject to persistent, warrantless observation—seems intuitively correct.[18]

The U.S. Supreme Court, the traditional protector of the public's right to "privacy,"[19] has historically had few, if any, satisfying responses to a

---

15. *E.g.*, Jamal Thalji, *Should Authorities Need a Warrant to Put a GPS Tracking Device On Your Car?*, ST. PETERSBURG TIMES, Oct. 20, 2010, *available at* http://www.tampabay.com/news/publicsafety/crime/article1128724.ece (discussing how the use of GPS tracking devices has lowered the standard required for searches and seizures under the Fourth Amendment of the United States Constitution); *see Jones*, 132 S. Ct. at 963–63 (Alito, J., concurring).

16. *See* Rehnquist, *supra* note 2, at 3.

17. *Id.* at 9.

18. *See* SLOBOGIN, *supra* note 2, at 110–13 (stating that empirical data tends to support the idea that freedom from public surveillance possesses support as a socially accepted norm). This study measured public opinions as to the perceived "intrusiveness" of several search and surveillance techniques. *Id.* at 111. Among them, the use of vehicle-borne GPS was rated as the fourteenth most intrusive practice on a list of twenty that were the subject of the survey. *See id.*

19. Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Action*, 102 MICH. L. REV. 801–04 (2004). Professor Kerr describes and criticizes the

public looking for protection from the dangers of a surveillance state. Whether it has been the use of beepers to track surveillance targets,[20] or police over-flights of private property,[21] the Court has historically held that these actions are not searches; therefore, they do not require warrants, because no definition of "privacy" in the constitutional sense could inure to a person when he or she exposes their conduct to public view.[22] Even when enhanced by technology, the philosophical question remains the same—how can someone reasonably expect to enjoy a sense of privacy even when in public?

Litigation in the appellate courts, manifesting itself in a debate over the particular technology of real-time Global Positioning System ("GPS") surveillance, has once again forced the issue as a problem for adjudication. Most federal appellate courts, in the context of recent GPS surveillance cases, have taken a conventional view that privacy, as a matter of Fourth Amendment doctrine, cannot logically expand into the public sphere.[23] The United States Court of Appeals for the District of Columbia, however, struck out in a substantially different direction, attempting to reevaluate settled law in light of new surveillance technologies. In *United States v. Maynard*, the court, sensing a similar problem as the one posed by Chief Justice Rehnquist, introduced the "mosaic theory," a conceptually novel approach to Fourth Amendment law intended to cultivate a constitutionally anchored sphere of privacy that would attach under conditions of long-term technology-driven surveillance operations.[24] According to the D.C. Circuit, persistent collection of publicly viewable conduct triggers Fourth Amendment scrutiny when such information can be aggregated into a "mosaic" that reveals essentially private insights about a person.[25] In the re-styled case of *United States v. Jones*, the Supreme Court had the opportunity to address directly the viability of the lower court's "mosaic theory" approach. De-

---

assumption that "the courts and the Constitution should offer the primary response" in matters of privacy and technology as the "popular view." *See id.* at 804.

20. *E.g.*, United States v. Knotts, 460 U.S. 276, 285 (1983).

21. *E.g.*,Florida v. Riley, 488 U.S. 445, 451–52 (1989); California v. Ciraolo, 476 U.S. 207, 215 (1986).

22. Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of *Fourth Amendment* protection.") (emphasis added).

23. *See, e.g.*, United States v. Marquez, 605 F.3d 604 (8th Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010); United States v. Garcia, 474 F.3d 994 (7th Cir. 2007).

24. *See* United States v. Maynard, 615 F.3d 544, 560–61 (D.C. Cir. 2010), *aff'd sub nom. Jones*, 132 S. Ct. at 954.

25. *See Maynard*, 615 F.3d at 560–62.

spite the Court's avoidance of the "mosaic theory" in its controlling rationale, a review of the *Jones* concurring opinions yields one remarkable and irreducible conclusion. The "mosaic theory," regardless of label, is conceptually alive and well as a source of future privacy litigation and policy-making.[26] With a majority of the Court having endorsed the normative assumptions and the analytical framework of the "mosaic theory,"[27] the complete canon of this litigation, from *Maynard* to its subsequent treatment in *Jones*, merits close discussion in order to gain a sense of how this doctrine might shape future constitutional doctrine and the governance of privacy policy in the context of surveillance technology. Critics of the *Maynard* "mosaic" have questioned whether Fourth Amendment privacy can, with any doctrinal coherence, expand so as to regulate government surveillance in plainly public areas.[28] Alternatively, even if such a rule can be ascribed to the Fourth Amendment, a question remains as to whether the Fourth Amendment should have to bear this weight or whether other policy responses would be more appropriate.[29] Answering these questions requires a review of the jurisprudential history of privacy and its doctrinal relationship with the Fourth Amendment.

THE FOURTH AMENDMENT BEFORE PRIVACY

Even though there is now a largely coterminous narrative between privacy and the Fourth Amendment, the more accurate textual and doctrinal starting point for this amendment is the determination as to whether an unreasonable search or seizure has taken place. When a claim of an illegal search is made, the Court starts by asking two questions which are textually grounded in the Fourth Amendment. As a threshold matter, the Court first asks whether the conduct is a "search."[30] If so, the Court then proceeds to

---

26. Orin Kerr, *What's the Status of the Mosaic Theory After Jones?*, THE VOLOKH CONSPIRACY (Jan. 23, 2012, 1:59 PM), http://volokh.com/2012/01/23/whats-the-status-of-the-mosaic-theory-after-jones/.

27. *See Jones*, 132 S. Ct. at 954–57 (Sotomayor, J., concurring); *see also id.* at 957–64 (Alito, J., concurring).

28. *See, e.g., D.C. Circuit Deems Warrantless Use of GPS Device and Unreasonable Search: United States v. Maynard*, 124 HARV. L. REV. 827 (2011); Orin Kerr, *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, THE VOLOKH CONSPIRACY (Aug. 6, 2010, 2:46 PM), http://volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search.

29. *See infra* Part V.C.3.

30. *E.g.*, Orin Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 528 (2007).

its second question, asking whether that conduct was reasonable.[31] Returning to the initial question, this threshold matter of finding a search is often determinative. For instance, if answered in the affirmative, the search, subject to a limited set of exceptions, is *per se* unreasonable unless conducted pursuant to a warrant based upon probable cause.[32] Conversely, answering this question in the negative has an equally powerful effect, as it means that any evidence obtained from activity which is not adjudged a "search" is *per se* reasonable and can be used at trial or for other law enforcement purposes.[33] What is also clear is that the inclusion of a "privacy" vocabulary into the analysis of searches and seizures is neither historically nor textually mandated in the Fourth Amendment, and the long, uneven debate as to whether and how to recognize Fourth Amendment rights as "privacy" rights reflects this tension. But as a jurisprudential matter, "privacy" is a court-recognized aspect of Fourth Amendment law, rather than a textually explicit one.[34] This means that the doctrinal concept must not only bear the constraints imposed by the amendment's text, but also those ascribed to it by the Court. Therefore, the only way to question strongly the settled doctrinal limits of "privacy" and how it relates to the public space is to get an accurate sense for how the term comes into use as a central feature of Fourth Amendment law.

THE "PRIVACIES OF LIFE" – BOYD V. UNITED STATES

In the modern era, the United States Supreme Court began this effort in 1886 with its decision in *Boyd v. United States*.[35] Prior to *Boyd*, the Fourth Amendment accumulated a significant amount of dust, as it remained "largely unexplored" territory.[36] The fact that this Amendment would lie dormant for so long after its enactment seems strange, as the concept of being free from illegal searches and seizures is so intertwined with early American history. In fact, an argument can be made that colonial contempt for searches and seizures executed pursuant to general writs of assistance, as illustrated by James Otis's resignation as advocate general in 1761 and subsequent court room orations against the Crown's use of gen-

31. *E.g.*, *id.*; *see, e.g.*, *Maynard*, 615 F.3d at 555.

32. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 31 (2001); Payton v. New York, 445 U.S. 573, 586 (1980); Katz v. United States, 389 U.S. 347, 357 (1967).

33. *See Four Levels of Fourth Amendment Protection*, *supra* note 30, at 528–29.

34. *See infra* Parts I–II.

35. *See* Boyd v. United States, 116 U.S. 616, 630 (1886).

36. WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE 126 (5th ed. 2009).

eral writs, sparked the intellectual and political will for revolution.[37] The lengthy period of dormancy, however, was probably less a function of cultural amnesia than a product of the Fourth Amendment's history and text.

As for text, the Fourth Amendment lacks a specified remedy for violation.[38] Contrast this with the Fifth Amendment, which textually implies an exclusion remedy, as a trial court would never allow a criminal defendant to be compelled to testify against himself.[39] Additionally, the historical context surrounding the Fourth Amendment may have tended to limit the conception of the rule in spite of its text. Consider that the Fourth Amendment textually contemplates the protection of not only houses from unreasonable searches and seizures but also persons, papers, and effects.[40] However, the historical record from the colonial period, acknowledged by the Court in *Boyd*, fixes on the specific problem of British officials breaking into homes for the purpose of seizing evidence of tax evasion or political sedition.[41] Unmooring the Fourth Amendment from this historically fixed perception, Justice Bradley writes for the Court:

> The principles laid down in this opinion affect the very essence of constitutional liberty and security . . . . [T]hey apply to all invasions on the part of the government and its employes [sic] of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property . . . . Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods, is within the condemnation of that judgment.[42]

What is especially remarkable about this opinion, however, is the introduction of life's "privacies"[43] into the discussion of the Fourth Amend-

---

37. *See Boyd*, 116 U.S. at 625 ("'Then and there,' said John Adams, 'then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born.'"); FREDERICK S. LANE , AMERICAN PRIVACY: THE 400-YEAR HISTORY OF OUR MOST CONTESTED RIGHT 11 (2009).

38. *See* U.S. CONST. amend. IV; LAFAVE ET AL., *supra* note 35, at 126. However, an exclusionary remedy was eventually recognized by the Court in *United State v. Weeks*, 232 U.S. 383 (1914), and subsequently extended to all non-federal law enforcement in *Mapp v. Ohio*, 367 U.S. 643 (1961). LAFAVE ET AL., *supra* note 36, at 126–27.

39. *See* U.S. CONST. amend. V; LAFAVE ET AL., *supra* note 36, at 126.

40. *See* U.S. CONST. amend. IV.

41. *See Boyd*, 116 U.S. at 624–25.

42. *Id.* at 630.

43. *Id.*

ment. Clearly, the Court contemplates that the notion of "privacy" they find in the Fourth Amendment includes the home and the ability to exclude government agents and others from invading it. But for them, illegal invasions of the "sanctity of a man's home" are only one concrete manifestation of the greater evil, which is the use of the government's power to break down the private barriers—the "privacies of life"—that foster individual liberty. Whether it is excluding the government from one's home or preventing the government from ordering the disclosure of mental processes in the form of compelled testimony, they perceive these barriers of exclusion as privacy interests rooted in the Fourth Amendment.[44]

So as the Court opens its modern discussion of the Fourth Amendment, there is a conversation that recognizes a tension between the amendment's express textual content, its historical context, and the sense that larger conceptual principles of privacy should be attributed to it. The difficulty, however, is to reconcile these potentially conflicting positions into constitutionally correct yet practically meaningful rules. *Boyd* and subsequent cases have no trouble constitutionally recognizing the intimate characteristics of the home. As James Otis described it, "[a] man's house is his castle; and whilst he is quiet, he is as well guarded as a prince in his castle."[45] But just as sure as the Court is that the Fourth Amendment creates an exclusionary right in the home and, in the specific case of *Boyd*, papers, they sense that a larger normative principle is present—privacy.

TRESPASS VERSUS DIGNITY – OLMSTEAD V. UNITED STATES

Four decades later, in *Olmstead v. United States*, the same conversation takes place in the context of electronic surveillance of the home.[46] In *Olmstead*, the appellant claimed that federal prohibition agents violated the Fourth Amendment when they intercepted phone conversations to and from his home.[47] The agent installed eavesdropping equipment to telephone lines exterior to his home.[48] Chief Justice Taft, writing for the Court, found

44. LAFAVE ET AL., *supra* note 36, at 126 (quoting *Boyd*, 116 U.S. at 633). Justice Bradley ultimately finds that the Fourth Amendment requires the textual assistance of the Fifth Amendment, writing that it had "been unable to perceive that the seizure of a man's private books and papers to be used against him is substantially different from compelling him to be a witness against himself." *Id.*

45. LANE, *supra* note 37, at 12.

46. *See* Olmstead v. United States, 277 U.S. 438, 473 (1928) (discussing how Fourth Amendment issues have far reaching implications involving privacy).

47. *Id.* at 455.

48. *Id.* at 457.

no Fourth Amendment violation. In light of the Fourth Amendment's text, he believed no violation could lie "unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' . . . ."[49] From Taft's perspective, the appellant's Fourth Amendment rights were limited to the power to physically exclude persons from intruding upon the interior and areas immediately adjacent to his home. Without trespass into these areas, however, no violation of the Fourth Amendment was present. Speaking directly to Justice Bradley's opinion in *Boyd*, Chief Justice Taft wrote that any belief in the need to liberally construe the Fourth Amendment so as "to effect the purpose of the framers . . . in the interest of liberty . . . [could] not justify enlargement of the language employed beyond the possible practical meaning of houses, persons, papers, and effects . . . ."[50] For Chief Justice Taft, once a person "projects" his voice over wires exterior to his home for the purpose of transmitting that message beyond the protected space of the home, he has lost the ability to control or exclude others from accessing it.[51] The Fourth Amendment does not provide a sweeping protection of the "privacies of life," but rather a right to control access and prevent others from physically intruding in and around the home.

In his well-known dissent, Justice Brandeis, citing to, and building upon the language in *Boyd*, continues the debate as to whether the Fourth Amendment is a rule solely controlled by a sense of tangible property boundaries or by broader concepts of privacy. Justice Brandeis identifies the surveillance in this case is something wholly different in character than the particular "evils" faced by Americans under British rule.[52] Presciently, he foresees a constant enhancement of surveillance technology at the inevitable cost of privacy that will ultimately give the government the ability to obtain and present in court "what is whispered in the closet," the contents of personal papers without ever removing them from drawers, and other "intimate occurrences of the home."[53] In fact, he even envisions "[a]dvances in the psychic and related sciences [that] may bring means of exploring unexpressed beliefs, thoughts and emotions."[54]

Predicting that these technological advances will quickly circumvent

49. *Id.* at 466.
50. *Id.* at 465.
51. *Id.* at 466.
52. *See Olmstead*, 277 U.S. at 473–75 (Brandeis, J., dissenting).
53. *Id.* at 473–74 (Brandeis, J., dissenting).
54. *Id.* at 474.

the Court's physical trespass rule, Justice Brandeis presents a highly personalized conception of the Fourth Amendment. His vision ties together concepts of human dignity to the privacy he envisions as a part of the Fourth Amendment.[55] With great eloquence, he writes:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations.[56]

This he famously describes as "the right to be let alone," in his opinion, the most valued right amongst civilized men.[57] But for all of the privacy and dignity-inspired verbiage Justice Brandeis employs, it is doubtful that even his vision of privacy can extend much beyond the barriers of the home. For instance, all of Justice Brandeis's proffered illustrations as to the capabilities of surveillance technology and the loss of privacy are envisaged as invasions of the home.[58] Though he speaks broadly of the founders looking to protect the value of one's life and individual dignity,[59] it is not at all clear, in light of the facts of the instant case and his illustrative scenarios,[60] that he perceives privacy as a right that can be enjoyed outside the home or without reference to some space reserved for private control and exclusion.

Even if an argument could be made that Justice Brandeis posited a view of privacy that includes spatial control over the elements of the mind,[61] making it a highly personal right that may transcend location, it is not at all clear that he would conceive of "the right to be left alone" as a right that prevents the government from observing conduct outside the home or from then gaining insights about one's mind as a result of such publicly available observation. What the *Olmstead* debate really questioned was whether the home possesses unique characteristics that warrant heightened privacy protection, even when a person waives some control

---

55. For an account of Fourth Amendment privacy as the preservation of individual dignity, *see* Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2094 (2001) (discussing JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 60–63 (2000)).

56. *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting).

57. *Id.*

58. *See id.* at 473–76.

59. *Id.* at 478.

60. *See id.* at 473–76.

61. *See id.* at 474–75, 478.

over his intellectual processes in the form of speech or other expression. Brandeis argued for a constructively impermeable barrier around the home; the majority rule limited the Fourth Amendment to a mere practical barrier. Neither side, however, suggested that speech or conduct outside the home could possess any claim of being "private" in a constitutionally recognizable sense.

PUBLIC VIEW – UNITED STATES V. LEE

Even if Justice Brandeis's dissent in *Olmstead* could be characterized as possessing some ambiguity as to whether he would find that individuals possess a sense of privacy so personal that it could extend into public spaces and receive constitutional protection from technological encroachment, his opinion in *United States v. Lee*,[62] written just one year prior to his *Olmstead* dissent, resolves the ambiguity against public notions of privacy. In *Lee*, a Coast Guard patrol boat chased down a suspected bootlegger off the coast of Massachusetts.[63] As the Coast Guard vessel approached the bootleggers, the ship's boatswain directed his spotlight at the suspicious vessel and saw what appeared to be crates of smuggled alcohol.[64] As a result, the Coast Guard officers seized the vessel and arrested the ship's crew.[65] The defendants claimed that the evidence obtained from the ship could not be used against them in court, because it was discovered and taken as a result of an illegal search and seizure.[66]

If this case had been decided subsequent to *Katz v. United States*, an interesting argument could have been made that the defendants, despite being in the most publicly accessible of spaces—the high seas—created for themselves a subjective expectation that their activities would remain undiscovered, which in a purely abstract sense is a form of privacy.[67] The smugglers traveled more than twenty miles off the coast in the middle of a foggy night.[68] Therefore, by exertion of natural, temporal, and spatial controls available to them, they purposely created a constructively private zone where public observation would almost certainly never occur. But for the use of surveillance technology—a searchlight mounted on a chase vessel in

62. United States v. Lee, 274 U.S. 559 (1927).
63. *Id.* at 560.
64. *Id.* at 561.
65. *Id.* at 560.
66. *Id.* at 561 (citing Weeks v. United States, 232 U.S. 383 (1914)).
67. *See infra* Part II.B.
68. *Lee*, 274 U.S. at 560.

this case—Coast Guard officials would not have been able to observe the cases of alcohol on the decks of the bootlegger's vessel.[69] However, in sharp contrast to the highly philosophical, privacy-oriented language employed in his *Olmstead* dissent, Justice Brandeis does not use the word privacy once in writing the *Lee* majority opinion.[70] Instead, he dismisses in the space of a few sentences the Fourth Amendment objection raised in *Lee*.[71]

For Justice Brandeis, there are only two facts of consequence. First, federal officers never had to look below decks to discover the bootlegged alcohol, as it was on deck and available for visual discovery without law enforcement boarding.[72] This portion of *Lee* is still controlling law and has since been translated into the oft-repeated proposition that "what a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[73] This single aphoristic proposition, founded in *Lee* and articulated forty years later in *Katz*, has since supported much of the Court's jurisprudence that privacy cannot be found in publicly observable space.[74] Second, the use of the search light in this case posed no constitutional problem as it was "comparable to the use of a marine glass or a field glass."[75] Citing to this portion of *Lee* some years later, the Court found that enhancing sensory perception through technology was of no constitutional consequence, because "[v]isual surveillance from public places . . . would have sufficed to reveal all of these facts to the police."[76]

The *Lee* opinion, read in combination with its subsequent application, sharply limits how one can view the Court's debate over privacy. Even though Justice Brandeis's *Olmstead* dissent argues for a broader, more personalized conception of privacy, he was ambiguous as to the specific spa-

69. *See id.* at 561.

70. *See id.* at 560–63.

71. *See id.*

72. *Id.* at 563

73. Katz v. United States, 389 U.S. 347, 351 (1967); LAFAVE ET AL., *supra* note 36, at 153.

74. WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE 56 n.49 (2nd ed. 1999) (quoting United States v. Dunn, 480 U.S. 294 (1987) ("[O]fficers' use of the beam of a flashlight, directed through the essentially open front of respondent's barn, did not transform their observations into an unreasonable search . . . ."); *see, e.g.*, California v. Ciraolo, 476 U.S. 207, 218–19 (1986) (Powell, J., dissenting) (citing *Katz*, 389 U.S. at 351); United States v. Knotts, 460 U.S. 267, 283 (1983) (discussing *Lee* in the context of Smith v. Maryland, 442 U.S. 735, 744–45 (1979), "[t]his analysis dictates that [Smith] can claim no legitimate expectation of privacy here. When he used his phone, [Smith] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business.").

75. *Lee*, 274 U.S. at 563.

76. *Knotts*, 460 U.S. at 282–83 (citing *Lee*, 274 U.S. at 563).

tial contours of this notion. However, when read in combination with his opinion in *Lee*, the ambiguity quickly recedes. Justice Brandeis would not attribute a right to privacy to any conduct that is observable in the public sphere, regardless of the advances in technology. Despite the substantial Fourth Amendment debate over privacy in *Olmstead*, the Court failed to consider whether any features of privacy can inure to the individual when in public. This strongly implies consensus among the leading Court members of the time that the constitutional notion of privacy is inconsistent with the public sphere. This holds true from the Court's perspective even when we as human beings exercise those natural controls available to use (such as distance, darkness, and time in the case of *Lee*)[77] to create a constructed sense of privacy in order to avoid public observation. And in all of this, technology made no analytical difference to the Court.[78]

THE TORTURED LIFE OF THE "TRESPASS RULE"

In the nearly four decades following *Olmstead* and preceding *Katz*, the debate over the Fourth Amendment's privacy characteristics quieted, as the Court continued to commit itself to the "trespass rule," a rule inconsistent with a conversation about privacy without reference to space.[79] *Goldman v. United States* demonstrated the Court's commitment, at that time, to adhere to, what it considered, a settled matter.[80] Federal agents placed the receiver of a listening device on their side of a wall shared with Goldman to record his conversations.[81] The recording device, a "detectaphone," did not physically penetrate, and, therefore, did not technically trespass, into Goldman's office.[82] In finding for the Government, the Court concluded:

> The petitioners ask us, if we are unable to distinguish *Olmstead v. United States*, to overrule it. This we are unwilling to do . . . . The views of the court, and of the dissenting justices, were expressed clearly and at length. To rehearse and reappraise . . . the conflicting views . . . would serve no good purpose. Nothing now can be profitably added to what was there said. It suffices to say that we adhere to the opinion there . . . expressed.[83]

---

77. *Lee*, at 560–61, 563.
78. *Id.* at 563.
79. *See, e.g.*, Goldman v. United States, 316 U.S. 129 (1942).
80. *See id.*
81. *See id.* at 131–32.
82. *Id.* at 131, 134–35.
83. *Id.* at 135–36 (adhering and refusing to overrule the decision in *Olmstead v. United States*, 277 U.S. 438 (1928), where the Court held that wire-tapping lines leading from the defen-

As this conclusion suggests, the preceding sections of the opinion offer little analysis in support of the *Olmstead* rule. Instead, as a matter of settled law, the Court simply refuses to disturb it. Despite Justice Murphy's attempt in dissent to forcefully re-introduce the language of privacy into the Court's discussion,[84] the remaining members, despite expressing reservations about the *Olmstead* rule, refused to re-open the question.[85]

Consequently, *Olmstead* continued forward as the rule; in doing so, making measurements of microphone penetration more constitutionally dispositive than normative debates of individual privacy.[86] But still, just as in *Goldman*, members of the Court, in both the majority and concurring opinions, continued to apply the *Olmstead* trespass rule only with a sense of unease as to its normative coherence with the Fourth Amendment.[87] For instance, in *Silverman v. United States*, a case where the Court measured the invasiveness of the now-infamous "spike mike,"[88] Justice Douglas, in his concurrence, asked, "[w]as not the wrong . . . done when the intimacies of the home were tapped, recorded, or revealed?"[89] Despite the majority's concerns, acknowledging that "Fourth Amendment rights are not inevitably measurable in terms . . . of ancient niceties of tort or real property law,"[90] the *Silverman* Court ultimately confirms its commitment to *Olmstead* and *Goldman*, expressly refusing to reconsider the trespass rule.[91] For the specific purpose of this discussion, the adherence to the "trespass" rule means that any notion of Fourth Amendment protection, attaching without reference to a constitutionally protected space, would have no persuasive purchase with the Court at this time. So long as *Olmstead* required "trespass" in order to maintain a Fourth Amendment objection, then *Lee* would re-

---

dants' residences to the chief office from which alleged conspiracy was orchestrated did not constitute an unlawful Fourth Amendment search or seizure, which would render evidence obtained by wire-tapping inadmissible).

84. *Id.* at 136–42 (Murphy, J., dissenting).

85. Goldman v. United States, 316 U.S. 129, 136 (1942) (Stone, C.J., and Frankfurter, J., concurring).

86. *See, e.g.*, Clinton v. Virginia, 377 U.S. 158, 158 (1964) (Clark, J., concurring) ("[T]he 'spiked' mike used by the police officers penetrated petitioner's premises sufficiently to be an actual trespass thereof . . . ."); Silverman v. United States, 365 U.S. 505, 511–12 (1961) (holding that intrusion into petitioner's "constitutionally protected area" by even a fraction of an inch was unconstitutional).

87. *See, e.g.*, *Silverman*, 365 U.S. 505.

88. *Id.* at 506–07.

89. *Id.* at 513 (Douglas, J., concurring).

90. *Id.* at 511 (citations omitted).

91. *Id.* at 512 ("We find no occasion to re-examine *Goldman* here, but we decline to go beyond it, by even a fraction of an inch.").

main strong precedent, preventing any possibility of constitutional protection to inure to activities accessible to "public view."

THE "PRIVACY" AMENDMENT – KATZ V. UNITED STATES

With the affirmation of the *Olmstead* trespass rule, the Fourth Amendment would continue to live in conflict with privacy as a normative goal. As the Court in the *Olmstead* era could not develop a coherent approach that integrated a concept of privacy into Fourth Amendment protection of the home—a space that enjoys express textual protection in the Constitution—a discussion on privacy characteristics outside the home was far outside the Court's analytical vocabulary. All of that dramatically changed with *Katz v. United States*.[92] In *Katz*, the Court underwent a dramatic paradigm shift, expressly incorporating the vocabulary of privacy into the Fourth Amendment.[93] Though *Katz* was not a case about privacy in public space *per se*, its newly introduced privacy-oriented approach, coupled with the specific factual posture of the case, created a jurisprudential foothold for a meaningful conversation about whether, or under what circumstances, an individual might possess some protection from government observation outside the home.

THE REASONABLE EXPECTATION OF PRIVACY: DECOUPLING PROPERTY FROM THE FOURTH AMENDMENT

The *Katz* Court drastically reconsidered the Fourth Amendment for the express purpose of protecting the privacy of individuals and not places.[94] In *Katz*, the Federal Government introduced evidence of the defendant's portion of a conversation recorded with the use of a microphone attached to the exterior of a phone booth, which the defendant frequently used.[95] After both the trial and appellate courts sustained the Federal Government's position regarding use of these recordings at trial, the defendant requested the Supreme Court's review. In doing so, the defendant invited the Court to re-consider *Olmstead* and *Goldman*, asking whether a right to privacy could attach to a conversation inside a telephone booth and, if so, whether physical penetration of that space was necessary in order to find a

92. 389 U.S. 347, 351 (1967).

93. *See infra* Part II.A–B; *Katz*, 389 U.S. at 353 (reasoning that listening to and recording a phone conversation violated the privacy and constituted a search and seizure within the meaning of the Fourth Amendment).

94. *See generally Katz*, 389 U.S. at 351.

95. *Id.* at 348.

Fourth Amendment violation.[96]

In answering the request, the Court discarded the premise that property law should determine whether the Government could search for and seize evidence in furtherance of a criminal investigation.[97] Instead, the Court expressly stated that the Fourth Amendment "protects people—and not simply areas . . . ."[98] With that shift, the Court made a serious interpretive decision and re-framed the issues presented in the case as follows: whether "[t]he Government's activities in electronically listening to and recording the [defendant]'s words violated the privacy upon which he justifiably relied while using the telephone booth . . . ."[99] Ultimately, the Court concluded that "one who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters . . . will not be broadcast to the world."[100]

However, despite its express interest in reorienting its Fourth Amendment jurisprudence towards a vocabulary of privacy, the Court took the position that "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'"[101] Due to the possibility that the Fourth Amendment can, in different scenarios, either fall short or go beyond what is necessary to protect normative concepts of privacy, the Fourth Amendment cannot fairly be characterized as a rule of privacy *per se*.[102] After the Court declined to interpret the Fourth Amendment as providing a generalized constitutional right to privacy, it described how it envisioned the making of privacy law in the United States by stating that "the protection of a person's general right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States."[103] Even though the express lan-

96. *Id.* at 349–50.

97. *Id.* at 353 (quoting Warden v. Hayden, 387 U.S. 294, 304 (1967)).

98. *Id.* at 353.

99. *Id.* at 353.

100. *Katz*, 389 U.S. at 352.

101. *Id.* at 350.

102. *See id.* at 350–51 n.4 (quoting Griswold v. Connecticut, 381 U.S. 479, 509 (1965) (Black, J., dissenting)). Distinguishing the Fourth Amendment's core concerns from a generalized right to privacy, the *Katz* Court stated:

> The average man would very likely not have his feelings soothed any more by having his property seized openly than by having it seized privately and by stealth . . . . [A] person can be just as much, if not more, irritated, annoyed and injured by an unceremonious public arrest by a policeman as he is by a seizure in the privacy of his office or home.

Id.

103. *Id.* at 350–51.

guage of this passage points to the States, it can be fairly read as saying that the protection of the general right to privacy should be left largely to policy-making institutions other than the courts. Having prefaced its discussion with the proposition that the Fourth Amendment only supports a textually limited species of privacy, the Court asserted that it was not the branch best suited to construct privacy policy. Despite the Court's attempt to demure in matters of privacy, its reorientation of Fourth Amendment doctrine has had the opposite effect. With the language of privacy made synonymous with the language of the Fourth Amendment, the Court ensconced itself as the branch of government perceived as primarily responsible for the creation and enforcement of privacy policy.[104]

In his concurrence, Justice Harlan articulated what is now oft-cited as the *Katz* test. As Justice Harlan understood the application of the majority's decision, two showings were required: first, that the defendant had an actual subjective expectation of privacy and that, second, the defendant's expectation was "one that society is willing to accept as 'reasonable.'"[105] Justice Harlan did not attempt to further define either element of this rule except to offer examples of what would not qualify. As to the first element, any conduct placed in the public sphere would indicate a lack of actual belief on the part of the actor that their movements were in any way private.[106] Second, even though a person may subjectively intend to maintain the privacy of some conduct or conversation placed in the public sphere, society is not, in Justice Harlan's view, prepared to accept those public activities as truly private.[107] As applied to the facts in *Katz*, Justice Harlan considered it inconsequential that the telephone booth could be used by other members of the public beyond the defendant.[108] Instead, he found it more important that this one particular place, though located in the public sphere, temporarily created for the user a reasonable belief that his conversation would be private, that is to say not subject to being overheard and recorded by non-participants to the conversation.[109] In a sense, by closing

104. *See The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Action*, *supra* note 19, at 803–04 ("While Congress and state legislatures may have a limited role regulating government investigations involving new technologies, the real work must be done by judicial interpretations of the Fourth Amendment. The courts come first, legislatures a distant second.").

105. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

106. *Id.* (reasoning that statements exposed to plain view are not protected because there was no intention to keep them private).

107. *Id.*

108. *Id.*

109. *See id.*

the door and paying the toll, the user not only exhibited a subjective belief that his conversation would remain private, but also created a constructively private sphere where society would recognize a right to exclude others from this conversation.

MEASURING PRIVACY AS "REASONABLE EXPECTATION"

Katz expressly tied the Fourth Amendment to normative notions of individual privacy. Despite the Court's assertions that the Fourth Amendment is not a rule of privacy, both the majority opinion and Justice Harlan's concurrence employed the language of privacy to determine whether a Fourth Amendment search had occurred. While shifting from a trespass to a privacy model of Fourth Amendment analysis clearly poses difficulties,[110] it was an ambitious attempt to offer a comprehensive, normative rule aimed at preserving Fourth Amendment principles in a world where the technological capabilities of surveillance seem only to steadily increase. Returning to Justice Harlan again, he justifies the Court's overruling of *Olmstead*, in part, because "[i]ts limitation on *Fourth Amendment* protection is, in the present day, bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic . . . invasion."[111] Though Justice Harlan offered no additional explanation regarding this sentence, it can be fairly read as an express concern that technological development would make the Fourth Amendment less relevant if applied through a "trespass" paradigm.

With this in mind, the Court discarded the talismanic "trespass" paradigm and replaced it with a rule that instead focused on what the Court considered the core policy concern underlying the Fourth Amendment—the individual privacy expectations that individuals must have in order to maintain a functioning and free society.[112] Though doctrinally imperfect as a matter of constitutional law, the "trespass" rule as a descriptive proxy for measuring the unreasonableness of government surveillance, at one time, had the practical effect of adequately protecting privacy in a world where the only way to access one's thoughts was to surreptitiously skulk and sneak around one's home and spy. With the advance of surveillance technology, however, the Court found it appropriate to dispense with the trespass rule as no longer effective for maintaining the vitality of the Fourth

110. LAFAVE ET AL., *supra* note 36, at § 3.2(a).
111. *Katz*, 389 U.S. at 362 (emphasis added).
112. LAFAVE ET AL., *supra* note 36, at § 3.2(a).

Amendment.

With the jurisprudential shift in *Katz*, freedom from surveillance would be tied to society's expectations of privacy. But an inquiry that searches for society's expectations of individual privacy can often have little empirical meaning, because it is not at all clear how to measure that societal expectation.[113] One potential measurement for gauging society's reasonable privacy expectations is assessing the frequency of public traffic in an area. In other words, if someone is conducting business in a place where there is a high likelihood of public discovery or observation, then maybe society is unprepared to accept that claim to privacy as justified or reasonable.[114]

However, under such a standard, persons similarly situated as those in the *Lee* case, having exercised the natural obscurants of time, place, and distance, could lay claim to a cognizable privacy expectation if mere "likelihood of discovery" is the application of the *Katz* rule.[115] Consider a hypothetical where two persons are either engaged in a drug deal or planning a domestic terrorist attack in a dark, secluded corner of Central Park at two o'clock in the morning.[116] Clearly, the persons engaged in this illicit meeting possess a subjective belief in their privacy, as evidenced by their use of remote location and time in combination with the cover of darkness. Instead of exerting control by virtue of property ownership, as formerly required by *Olmstead*, they are preventing observation through various natural controls, including temporal (middle of the night), spatial (abandoned corner in a parker), and visual (cover of darkness). In light of those controls, one could argue, just as in *Lee*, that the time and location of this transaction creates both a subjective (clearly attempting to avoid observation) as well as an objective (a high likelihood that they will succeed in avoiding observation) expectation of privacy. Using this logic, any conduct that takes place in a remote portion of Central Park at a time of low traffic volume under the cover of darkness could potentially qualify as private, so long as one could reasonably expect to avoid public observation. Even though the park is in one sense as public as the telephone booth in *Katz*, it is also at least as private in this abstract sense. The pay phone and the park only differ in terms of the control mechanisms employed—one has a door, walls, a phone line, and requires a toll, while the other employs

113. United States v. White, 401 U.S. 745, 769–95 (1971) (Harlan, J., dissenting).
114. LAFAVE ET AL., *supra* note 36, at § 3.2(a).
115. *See supra* Part II.B.
116. LAFAVE ET AL., *supra* note 36, at § 3.2(a).

space, position, darkness, and time. The rule from *Katz* then, especially when read in the specific context of its facts, permits the concept of public privacy to enter the conversation.

However, as a policy matter, that result would seem untenable, as it would create for criminals or plotting terrorists, through successful employment of detection countermeasures, an expectation of privacy in public spaces. This would frustrate society's legitimate interest in enforcing its laws and maintaining its national security.[117] That impossible result cannot be one that society is willing to recognize as reasonable. The Court, therefore, must have been looking to something more qualitatively robust than a mere calculation as to the chances of someone getting caught. Otherwise, criminals or terrorists would be rewarded with bubbles of quasi-privacy for being tactically proficient at evading detection.

Recognizing this logical hole in *Katz*, while still attempting to realize the normative benefits of the *Katz* rule, Justice Harlan, in his dissent in *United States v. White*, suggested that the character of both the action being taken by government and the actions of the individual member of society be judged and balanced in order to measure the reasonableness of the investigative practice. Specifically, Justice Harlan envisioned the formula as follows:

> This question must, in my view, be answered by assessing the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement. For those more extensive intrusions that significantly jeopardize the sense of security which is the paramount concern of *Fourth Amendment* liberties, I am of the view that more than self-restraint by law enforcement officials is required and at the least warrants should be necessary.[118]

What this test amounts to, as described by Professor Amsterdam, is a "value judgment."[119] More specifically, Professor Amsterdam articulates the balance as "whether, if the particular form of surveillance . . . is permitted to go unregulated by constitutional restraints, the amount of privacy and

---

117. Christopher Slobogin & Joseph 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, 731 (1993) (quoting Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978)). "According to the Court, the use of the word 'legitimate' or 'reasonable' before 'expectations of privacy' is meant to convey 'more than a subjective expectation of not being discovered.'" *Id.*

118. *White*, 769 U.S. at 786–87 (Harlan, J., dissenting) (emphasis added).

119. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974).

freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society."[120] For example, if society is unprepared to recognize a privacy interest in well-concealed criminal conduct, society may be similarly unprepared to sanction overly intrusive government responses that cause innocent persons, not engaging in any type of criminal conduct, to have to constantly guard themselves from observation.[121]

If the question after *Katz* truly was a pure balancing of competing values, this would have amounted to a substantial paradigm shift in Fourth Amendment analysis from the *Olmstead* rule. However, *Katz* has rarely been applied in such normative abstraction. To the contrary, for reasons consistent with the practical needs of law enforcement and society, the Court has tended to favor a return to descriptive rules that have tangible reference points for measuring society's privacy expectations.[122] For instance, in *Rakas v. Illinois*, the Court explicitly reintroduced notions of property law into the Fourth Amendment in order to determine the presence of an objective expectation of privacy.[123] Meaning that, despite being couched in the normative language of privacy from *Katz*, the debate has since more closely resembled the one from the *Olmstead* era—an assessment of the ability to control and exclude observation premised upon established notions of property law.

SURVEILLANCE TECHNOLOGY AND THE PUBLIC/PRIVATE BOUNDARY

As the jurisprudential language of privacy has receded from the

120. *Id.*

121. *Id.*

122. *See Four Models of Fourth Amendment Protection, supra* note 30, at 528–29.

123. Rakas v. Illinois, 439 U.S. 128, 143 (1978). The *Rakas* Court held:

> Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society. . . . But by focusing on legitimate expectations of privacy in Fourth Amendment jurisprudence, the Court has not altogether abandoned use of property concepts in determining the presence or absence of the privacy interests protected by that Amendment. No better demonstration of this proposition exists than the decision in *Alderman v. United States*, 394 U.S. 165 (1969), where the Court held that an individual's property interest in his own home was so great as to allow him to object to electronic surveillance of conversations emanating from his home, even though he himself was not a party to the conversations. On the other hand, even a property interest in premises may not be sufficient to establish a legitimate expectation of privacy with respect to particular items located on the premises or activity conducted thereon.

Id.

Court's Fourth Amendment doctrine, the natural consequence has been that surveillance technologies that collect information in space external to the home have continued to advance. Developers of surveillance technology have moved to exploit this space, because the Supreme Court's post-*Katz* jurisprudence has created an external sphere where information collection can occur with almost no judicial oversight. The Court's Fourth Amendment architecture since *Katz* has incentivized the development of surveillance tactics, techniques, and technologies that avoid judicial observation while still permitting law enforcement to collect and collate large volumes of information about investigatory targets. Therefore, the rise of surveillance technology and the question of reasonable expectations of privacy in the public sphere go hand-in-hand. The regulatory incentives that have led to the increased development and deployment of surveillance technologies can best be illustrated by reviewing the Court's treatment of two older surveillance technologies—beeper tracking and manned aerial surveillance—and then assessing their subsequent enhancement and expanded use in response to the Court's decisions.

PRIVACY ON PUBLIC STREETS: UNITED STATES V. KNOTTS AND "BEEPER" TRACKING

In *United States v. Knotts*, the Court reviewed the constitutionality of surveillance conducted with a beeper tracking device.[124] Although the Court ultimately found no Fourth Amendment violation in the warrantless use of beeper tracking devices,[125] the opinion acknowledged the possibility that technologically enhanced surveillance, even when conducted in public spaces, may not always survive constitutional scrutiny.[126] In this case, law enforcement suspected three individuals of making methamphetamines, and arranged to have a tracking device (a "beeper") placed in a barrel of chloroform, a methamphetamine precursor. [127] The beeper-loaded chloroform barrel was subsequently purchased by a suspected conspirator.[128] While police tracked the suspect visually at the outset, they also tracked the suspect remotely with the assistance of the beeper.[129]

---

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

125. *Id.* at 285 (finding that monitoring beeper signals did not intrude upon a legitimate expectation of privacy).

126. *Id.* at 283–84 (stating that if the surveillance should be abused by law enforcement, the Court will find time to return to the topic and determine its constitutionality).

127. *Id.* at 277.

128. *Id.* at 278.

129. *Id.* at 278. "A beeper is a radio transmitter, usually battery operated, which emits peri-

Even though the operation began as visual surveillance, the beeper's tracking capability later became critical as agents lost visual observation of the vehicle. With the assistance of remote beeper monitoring, agents re-established visual observation and discovered the location of the group's methamphetamine laboratory at the defendant's home.[130] According to the Court, the record indicated no subsequent uses of the beeper, finding its use was limited to this single, day-long operation.[131]

Consistent with its modern application of *Katz*, the Court began its analysis in *Knotts* with the familiar acknowledgment of the personal quality of the Fourth Amendment's protections.[132] The Court, however, quickly moved from this general statement and more descriptively styled the question as whether the defendant had any objective expectation of privacy in his movements from one place to another on public streets.[133] The Court found that no such expectation attached to the defendant's activities in this case, characterizing travel over public roads as implying permission to be observed by anyone who may have the physical capability to do so.[134] Because the defendant chose to be present in the public eye, he implicitly acquiesced to any and all observation of his conduct by any person who had the interest or the capability to do so, including law enforcement.[135] This included the subsequent tracking of the barrel's movements on his property, as the defendant had no expectation of privacy in its movement in the observable "open fields" outside his home.[136]

Although the facts of this case only deal with one specific surveillance technology, the Court's treatment of this issue implied a broader rule which would make the use of other visual surveillance technologies almost universally permissible when employed in space outside the home. In *Knotts*, the Court found the use of beeper tracking technology of little constitutional consequence, because surveillance technology in general, raises no concern separate from the assessment of the underlying surveillance activity.[137] From the Court's perspective, if visual surveillance from a public

odic signals that can be picked up by radio receiver." *Id.* at 277.

130. *Knotts*, 460 U.S. at 278.

131. *Id.* at 284–85.

132. *Id.* at 280 (finding that "the Fourth Amendment depends on whether the person invoking its protection can claim" a reasonable expectation of privacy).

133. *Id.* at 281–82.

134. *Id.*

135. *See id.* at 281–82 (finding that defendant "voluntarily conveys" his direction of movement to anyone who chooses to look at him while he is in public).

136. *Knotts*, 460 U.S. at 282 (citing Hester v. United States, 265 U.S. 57, 59 (1924)).

137. *Id.* at 282–83 (quoting United States v. Lee, 274 U.S. 559, 563 (1927)).

place could have revealed the same information as the beeper, then "[n]othing in the *Fourth Amendment* prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them . . . ."[138] As in *Lee*, shining a light on the deck of a boat at night to determine the presence of bootlegged liquor does not implicate the Fourth Amendment, because, but for the lack of sun light, the deck of a boat is open to the observation of any passing vessel.[139]

Analogous to the observation of a ship's deck with a light, the Court found that "beepers are merely a more effective means of observing what is already public."[140] From the Court's perspective, enhancement to visual surveillance raises no constitutional issue which is not raised by the conduct of the underlying surveillance.[141] Therefore, because all of the defendants' movements were susceptible to observation from a publicly available vantage point, technological enhancement which simply makes visual surveillance or even data surveillance more efficient or effective raises no constitutional objection.

After reaching this conclusion, the Court addressed the defendant's objection that such a permissive view, if applied to its logical extreme, would effectively sanction persistent, "dragnet" surveillance of any person or place without judicial oversight, so long as the suspected criminal activity targeted for surveillance was susceptible to observation from a publicly accessible space.[142] This result would compel a rule that all surveillance conducted from public space is *per se* reasonable and requires no additional Fourth Amendment scrutiny or judicial oversight. In other words, means of collection would truly make no difference, because all information is constructively exposed when it is susceptible to observation or collection from a publicly accessible location. The consequence of this logic would be the effective removal of visual surveillance, regardless of technological en-

138. *Id.* at 282.

139. *Id.* at 283 (quoting *Lee*, 274 U.S. at 563 (1927). The *Knotts* Court stated:

> But no search on the high seas is shown. The testimony of the boatswain shows that he used a searchlight. It is not shown that there was any exploration below decks or under hatches. For aught that appears, the cases of liquor were on deck and, like the defendants, were discovered before the motor boat was boarded. Such use of a searchlight is comparable to the use of a marine glass or a field glass. It is not prohibited by the Constitution.

Id.

140. *Id.* at 284.

141. *Id.* at 282.

142. *Knotts*, 460 U.S. at 283–84.

hancement, from the ambit of the Fourth Amendment altogether, thus reducing reasonable expectations of privacy in the context of surveillance to a mere practical game of technological abilities and countermeasures.

In response, the Court commented that these concerns are merely speculative as "the reality hardly suggests abuse."[143] However, not completely dismissing the concerns raised, the Court expressly reserved the issue for future consideration, concluding that if "dragnet-type" investigatory techniques should occur, that "there will be time enough then to determine whether different constitutional principles may be applicable."[144] Until that future time, however, the Court would decline to take any measures that might be construed as *per se* equating enhanced surveillance efficiency with unconstitutionality.[145]

PRIVACY AND AERIAL VIEW

While cases such as *Lee* and *Knotts* establish the basic doctrinal premise that privacy cannot exist in areas accessible to public view, what they do not establish well is the boundary at which "public view" or public space ceases and the power to exclude begins. The boundary determination problem, in one sense, returns us to the debate between Taft and Brandeis in *Olmstead.* While Brandeis might argue that the home is a place that must be constructively preserved from "public view" by virtue of its identity as "the home," Taft would have likely argued that the home is only as private as the actual exclusion successfully exercised by its resident. In its specific treatment of aerial surveillance, a technology which tests constitutional assumptions about location, observation, and the power to exclude observation, the Court endorsed the series of principles that would continue to permit surveillance technology to constrict and define for itself the constitutional boundaries of the "private" versus the "public."

Open Fields: Oliver v. United States

While *California v. Ciraolo* and *Florida v. Riley* are technology specific cases in the analysis of aerial surveillance, they are doctrinally a subset of a larger jurisprudence pertaining to the concepts of curtilage and "open fields."[146] In *Oliver v. United States*, the Court sets the stage for its

143. *Id.* at 283–84 (quoting Zurcher v. Stanford Daily, 436 U.S. 547, 566 (1978)).
144. *Id.* at 284.
145. *Id.*
146. Florida v. Riley, 488 U.S. 445, 451–52 (1989) (holding an officer's observation of the

subsequent treatment of surveillance by granting broad authority to surveil "open fields" without a warrant.[147]

What makes *Oliver* particularly important in this context is that the Court, in its discussion of an "open field" search, anticipated the question of aerial surveillance. In *Oliver*, law enforcement acted on a tip that the petitioner was growing marijuana.[148] Undeterred by a "No Trespassing" sign, the police walked onto the petitioner's property, eventually finding marijuana plants being grown.[149] Though the petitioner lived on the farm property, the plants were not grown immediately near his home.[150] Instead, they were on a piece of the petitioner's land located nearly a mile from his mobile home.[151] Despite the technical trespass, the Court concluded that officers had not violated the Fourth Amendment when they entered the petitioner's farm property in order to look for marijuana.[152]

Tying the open fields doctrine squarely to its post-*Katz* jurisprudence, the Court held that "an individual may not legitimately demand privacy for activities conducted out of doors in fields, except in the area immediately surrounding the home."[153] According to the Court, the curtilage should continue to be treated as a part of the home for Fourth Amendment purposes, because of its requisite characteristics in relation to the home. In other words, the curtilage receives Fourth Amendment protection "by reference to the factors that determine whether an individual reasonably may expect that an area immediately adjacent to the home will remain private."[154]

An "open field," on the other hand, being outside the curtilage, offers no such legitimate expectation of freedom from warrantless government intrusion.[155] That is why, despite the apparent trespass by the officers in

---

interior of a partially covered greenhouse from the vantage point of a helicopter did not constitute a "search" for which a warrant was required); California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding that a warrantless aerial observation of a fenced-in backyard within the curtilage of the home was not unreasonable under the Fourth Amendment).

147. Oliver v. United States, 466 U.S. 170, 183–84 (1984) (holding that the "open fields" doctrine was applicable in determining whether the discovery or seizure of marijuana in question was valid).

148. *Id.* at 173–74.

149. *Id.* at 173.

150. *Id.*

151. *Id.*

152. *See id.* at 183–84 (finding that trespass to property is only one element to be considered in establishing a legitimate expectation of privacy pursuant to the Fourth Amendment).

153. *Oliver*, 466 U.S. at 178.

154. *Id.* at 180.

155. *Id.* at 179.

Oliver, no constitutional violation was found. The Court then noted that to accord some heightened expectation of privacy to open fields would merely create a rule that requires law enforcement to survey open fields by way of aerial surveillance, which the Court seems to assume would be perfectly permissible in the case of an open field because of its diminished indicia of privacy.[156] The Court concluded that such a proposed rule, therefore, would not advance privacy interests if all it dictated was that an aerial vantage point could circumvent the "open field" privacy interest posited by the petitioner.[157] As a result of this *dicta*, *Oliver* became not only a defining "open fields" and "plain view" case, but also, in a sense, the first aerial surveillance case, strongly signaling its approval of such observation tactics. With open fields expressly removed from the Fourth Amendment's protection, the next question that would arise was whether, and to what degree, aerial surveillance could continue to alter expectations of privacy in areas in the immediate vicinity of the home.

Aerial Surveillance: *Ciraolo* and *Riley*

In both *California v. Ciraolo* and *Florida v. Riley*, the Court applied its "open fields" and "public view" jurisprudence to their logical extremes and continued to endorse the broadest view of government self-regulation of surveillance technology. In *Ciraolo*, law enforcement flew a plane over the defendant's property at an elevation of 1,000 feet in navigable air space and identified marijuana plants being grown in his backyard.[158] Citing *Oliver*, the defendant claimed that because his yard was within the curtilage of his home, any aerial observation without a warrant violated the Fourth Amendment.[159] However, the Court found the defendant's claimed expectation of privacy unreasonable. In the Court's opinion, so long as law enforcement officers could make their observations from a publicly accessible vantage point,[160] then the defendant had placed his property in "plain view" and no reasonable expectation of privacy could attach.[161] Of critical importance to the Court was the public's use of the nation's air space. The Court found that the defendant could not reasonably expect his yard to be free

156. *Id.* at 179 n.9.
157. *Id.*
158. California v. Ciraolo, 476 U.S. 207, 209 (1986).
159. *Id.* at 212 (citing *Oliver*, 466 U.S. at 180).
160. *Id.* at 213–14.
161. *See id.* at 215 (promulgating that anything exposed in plain view is not protected because such exposure precludes an intention on behalf of an individual to keep an object out of the public arena).

from aerial observation, because members of the public had reasonable access to the airspace over his home.[162] Therefore, because the defendant should anticipate the public's lawful presence in the air space above his home, then "[t]he *Fourth Amendment* simply does not require the police traveling in the public airways . . . to obtain a warrant in order to observe what is visible to the naked eye."[163]

In dissent, Justice Powell accused the majority of ignoring the central concern underlying *Katz*—the rise of surveillance technology. In his opinion, Justice Powell contends that the majority's decision would re-establish the Fourth Amendment as a rule which only proscribes physical trespass.[164] Instead, he reminds the Court that, as Justice Harlan had warned in *Katz*, enhanced surveillance technologies can defeat privacy expectations to the same or greater degree than physical trespasses.[165] Employing sophisticated aviation technology, the police successfully exploited a completely new piece of maneuver space. While technically accessible to the public, it is in no way public in the same sense as a street or a sidewalk is.[166] To say that individuals, even in the privacy of their homes, should reasonably expect to be observed by the occasional passerby on adjacent streets or sidewalks does not at all translate into a similar expectation of observation from commercial aviation passengers, flying thousands of feet in the air at hundreds of miles per hour, simply because of their lawful, physical presence in that space.[167]

Despite Justice Powell's arguments, a majority of the Court found the surveillance in *Ciraolo* to be constitutionally reasonable, because the police, though assisted by aviation technology, were lawfully present in that aerial vantage point.[168] However, not all aviation platforms present identical capabilities and concerns.[169] While fixed-wing platforms, like the one employed in *Ciraolo*, offer effective aerial surveillance, rotary aviation can provide uniquely precise surveillance capability.[170] Despite the heightened

162. *See generally id.*
163. *Id.* at 215 (emphasis added).
164. *Ciraolo*, 476 U.S. at 215–16 (Powell, J., dissenting).
165. *See id.*
166. *See id.* at 218, 223–25.
167. *See id.* at 223–24.
168. *Id.* at 215.
169. *See* JULIE K. PETERSEN, UNDERSTANDING SURVEILLANCE TECHNOLOGIES: SPY DEVICES, THEIR ORIGINS & APPLICATIONS 9-6 (2001) ("A variety of aerial craft are used in civilian and aviation surveillance including light planes, helicopters, and remote-controlled aircraft.").
170. *See* BARRY DAVIES, THE SPYCRAFT MANUAL: THE INSIDER'S GUIDE TO ESPIONAGE TECHNIQUES 58 (2005) ("Helicopter surveillance has become popular with the police as it pro-

potential intrusiveness of rotary surveillance, the Court, only a few years after *Ciraolo*, concluded that there was no reasonable expectation to be free from warrantless helicopter surveillance of the home and its curtilage.[171]

In *Florida v. Riley*, local law enforcement found themselves in a similar situation as the police in *Ciraolo*,[172] except that police used a helicopter to conduct aerial surveillance at an altitude of only 400 feet.[173] Making two passes over the property, police saw a partially uncovered greenhouse that had marijuana plants growing inside.[174] In a plurality opinion, five members of the Court found the conduct of unwarranted helicopter surveillance constitutionally permissible.[175]

The dissenting members of the Court echoed many of the concerns voiced in previous aerial surveillance cases.[176] They found unpersuasive the attempt to analogize aerial surveillance with surveillance from a public road or sidewalk, based upon the notion that in both instances the observer was lawfully present in each vantage point.[177] The constitutional fault in the analogy, according to the dissent, is the result of the heightened technological advantage.[178] The police, as a result of having ready access to an expensive and sophisticated piece of equipment, can access air space with an ease and frequency that few ordinary citizens can.[179] In other words, according to the dissent, to say that the defendant's property was in public view is really to say that the defendant had a reasonable expectation that the public would actually view his property from the air.[180] Of course, from the dissent's perspective, this is clearly not the case. In their view, the appropriate test would be to ask, "[w]hether [the] public observation of Riley's curtilage was so commonplace that Riley's expectation of privacy in

---

vides an overt observation platform for many different operations . . . . Helicopters have the advantage of speed and unrestricted progress while in the air, making them ideal for: surveillance, [and] aerial photography . . . ."); LARRY K. GAINES & VICTOR E. KAPPELER, POLICING IN AMERICA 181–82 (7th ed. 2011) ("[L]arge[] and medium-sized police departments have large numbers of aircraft, with eighty-eight percent having helicopters and forty percent having fixed-wing aircraft . . . . Helicopters are more prevalent than airplanes because of their versatility in surveillance and support activities.") (citation omitted).

171. *See* Florida v. Riley, 488 U.S. 445, 450–52 (1989).
172. *See id.*
173. *Id.* at 448.
174. *Id.*
175. *Id.* at 455 (O'Connor, J., concurring), 450 (plurality opinion).
176. *See id.* at 456–65 (Brennan, J., dissenting).
177. *Riley*, 488 U.S. at 459–60.
178. *See id.* at 460.
179. *See id.*
180. *See id.*

his backyard could not be considered reasonable."[181]

PROPERTY AND THE RIGHT TO EXCLUDE TECHNOLOGY-BASED SURVEILLANCE: KYLLO V. UNITED STATES

When read together, the *Knotts* and *Ciraolo/Riley* precedential lines create a remarkable picture of how the post-*Katz* Supreme Court viewed privacy. First, *Knotts* established the basic inside-outside distinction that defines constitutional privacy relative to space.[182] In simplest terms, *Knotts* stands for the basic proposition that inside is private while outside is not.[183] Following shortly after *Knotts*, the Court constricted the inside-outside boundary further with its subsequent aerial surveillance cases. With *Ciraolo* and *Riley*, the Court constrained the private sphere further by allowing technological capability to pursue and define its own constitutional legitimacy. Though decided in the specific factual context of aerial surveillance, these decisions strongly suggest that anything which could be seen from an accessible vantage point was "outside" and no longer private. Therefore, so long as the observer was in a lawfully obtained vantage point, technology could continue to push into traditionally regarded private spaces by bringing more activity constructively "outside," thereby stripping even traditionally private areas of any Fourth Amendment recognition.

The implications of these cases came to fruition quickly, as they coincided with the subsequent deployment of enhanced technologies, such as GPS, Unmanned Aircraft Systems ("UAS"), and thermal imagery devices. For instance, until the Court decided *United States v. Kyllo*, the majority of lower courts had continued to apply these surveillance-permissive principles to the their logical extreme, finding permissible the use of thermal imagery even against the home, premising such a conclusion on the theory that heat waves were "exposed" to public collection.[184] This meant that

181. *Id.*

182. United States v. Knotts, 460 U.S. 276, 281–82 (1983) (reasoning that a person does not have a reasonable expectation of privacy while travelling outside on public thoroughfares, but a person does have a traditional expectation of privacy inside a private dwelling); *see D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, *supra* note 28 ("In Fourth Amendment law, stuff inside—inside homes . . . and hidden from public view—is generally protected. In contrast, stuff outside—stuff exposed to the public—is not protected."); *supra* Part III.A–B (discussing the *Knotts* inside-outside distinction).

183. *Knotts*, 460 U.S. at 281–82; *see also D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, *supra* note 28 (explaining that *inside* is generally protected by a reasonable expectation of privacy, but *outside* is not).

184. SLOBOGIN, *supra* note 2, at 51 (citation omitted); *see infra* Part III.C. (quoting Justice Scalia in *Kyllo* as saying that any information regarding the interior of the home obtained through

courts were effectively allowing technology to draw activities from the interior of the home to its exterior, thereby exposing them as a matter of constitutional doctrine to "public view" and observation. In this atmosphere of doctrinal instability, where constitutional doctrine had been applied to a seemingly corrosive extreme, the Court in *Kyllo* attempted to impede the ability of surveillance technology to unilaterally regulate the boundaries of privacy.

Even though *Kyllo* is neither a beeper monitoring case, nor an aerial surveillance case, it is a case critical to the discussion of understanding how technology can push the boundary between the public and private to its absolute limit. In finding that surveillance of the home with a thermal imagery device was a search, Justice Scalia began with a brief, though telling, historical review of visual surveillance law.[185] Implying a desire to return to the "trespass" doctrine, Justice Scalia described how the question of what constitutes a search was no longer as "clear" as it once was when *Olmstead* and its progeny were the law.[186] Under the *Olmstead* approach, the rule would have been clear, as "the eye cannot . . . be guilty of trespass."[187] Quoting from *Ciraolo*, he remarked that "the Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."[188] Regardless of his nostalgia for a simpler time when questions of property were dispositive, he eventually engaged the *Katz* test. Justice Scalia posited that visual observation of the home would not be a search, unless the resident had manifested some subjective expectation of privacy that society was willing to protect.[189] Justice Scalia's articulation of this principle emphasizes a slightly different, yet consequential aspect of the *Katz* rule. For Justice Scalia, a place (in this instance, the home) merely offers a constitutionally cognizable (in other words, objective) authority to exclude public observation. However, unless the individual exercises that exclusionary right through some action (i.e., drawing curtains, building enclosures, shutting the door) then no subjective expectation of privacy has been manifested. In *Kyllo*, the Court affirms a conception of privacy that is measured neither by place nor by action alone. Rather, they are concepts

---

sense-enhancing technology is not general public use and not protected by the Fourth Amendment to the United States Constitution).

185. Kyllo v. United States, 533 U.S. 27, 31–33 (2001).

186. *Id.*

187. *Id.* at 32 (quoting Boyd v. United States, 116 U.S. 616, 628 (1886)).

188. *Id.* (quoting California v. Ciraolo, 476 U.S. 207, 213 (1986)).

189. *Id.* at 33 (citing *Ciraolo*, 476 U.S. at 211).

which work in tandem with place representing the objective side of the analysis and action the subjective.

Even though constitutional privacy can be viewed as the intersection of place and exclusion, there are certainly others areas that, though not strictly protected by constitutional rule, people once thought of and considered private in a normative sense. Justice Scalia tacitly conceded that technological advances have shrunk society's zone of expected privacy down to only those that that are constitutionally enumerated.[190] He cited to the proliferation of aviation surveillance as a specific example of how technology has exposed to public view one's backyard, even though that was formerly thought of as private.[191] However, he distinguished the interior of the home as a qualitatively different space that could resist encroachment.[192] For Justice Scalia, the Fourth Amendment warrant requirement was triggered in *Kyllo* once the government:

> [o]btain[ed] by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area" . . . at least where (as here) the technology in question is *not in general public use.*[193]

Initially, the rule affirms that the interior of the home is normatively different than areas exterior to the home that may be in public view. However, at the same time, it then drills a technological hole into the walls of the home with the insertion of the "general public use" test.[194] Despite the objectively recognized authority to exclude observation of oneself when inside the home, Justice Scalia found that technologies, once in "general public use," may gain access to the interior of the home in a way that would otherwise require a warrant. *Kyllo*'s approach to demarcating the line between public versus private can be interpreted as a survey of the technological marketplace.[195] Though Justice Scalia cited to no case, constitutional amendment, or statute for the "general public use" exception, he could have cited to the majority opinion in *Olmstead*, as the logic is not dissimilar.[196] The "general public use" exception, if ever zealously pursued by the gov-

190. *Id.* at 33–34.

191. *Kyllo*, 533 U.S. at 33 (citing two cases where aerial surveillance of private homes does not constitute a search).

192. *Id.* at 34 (citing Silverman v. United States, 365 U.S. 505, 512 (1961)).

193. *Id.* (quoting *Silverman*, 365 U.S. at 512) (emphasis added).

194. *Id.* (establishing a general public use requirement for technology used to gather information regarding the inside of a house).

195. *See, e.g.*, SLOBOGIN, *supra* note 2, at 55–57.

196. *See supra* Part I.B.

ernment, would re-introduce in principle the logic of trespass into the Fourth Amendment. To allow technology an opportunity to pierce the interior of the home would diminish its objective value as a place where individuals possess a unique constitutional authority to remove themselves from public or government observation. As the normative privacy value of the home diminishes, this transforms the Fourth Amendment into a mere consequential review of the practical state of surveillance technologies. So whether the technology is aviation, imagery, or location tracking, as they become less expensive, more convenient, and more available to the general public, then the places that the Court will recognize as providing some opportunity for privacy would likely recede under this rule.

Even though *Kyllo* potentially hollowed out the exclusionary force of the home with the "general public use" exception, it explicitly reinforced a point originally observed by the Court going as far back as *Olmstead*—that constitutional privacy cannot inure without reference to location. Though commentators may debate how and to what degree the "general public use" exception might continue to destabilize Fourth Amendment jurisprudence, what is clear for the purpose of this discussion is that the Court in *Kyllo* cannot conceive of privacy attaching without spatial reference to a place that offers a constitutionally cognizable right to exclude public observation. Of course, confirming the importance of location in our analysis works in direct opposition to any attempt to articulate a right to privacy-like attributes existing in the public sphere. If assessing location is important, that must mean that some places must not qualify as "private," otherwise nothing would seemingly be excluded from it. From the analytical viewpoint of *Kyllo* and preceding cases, a conceptual space described as "private" can only exist in contrast to an alternative state—the "public"—which necessarily cannot be included. Without such distinction, the concept of the "private" would seem to collapse. But as both Chief Justice Rehnquist and Justice Scalia have observed at different times, recognizing a constitutional distinction between "public" and "private" provides little satisfaction to a citizenry that senses the encroachment of observational technology on what they have always perceived as a moral right to a privately lived life.[197]

NEW SURVEILLANCE TECHNOLOGIES AND THE DEMAND FOR "PUBLIC PRIVACY"

Despite the logical conclusion that the "public" cannot be "private,"

197. *See* SLOBOGIN, *supra* note 2, at 31; ALAN F. WESTIN, PRIVACY AND FREEDOM 31 (1967).

there still seems to be the sense, recalling the Rehnquist hypothetical, that a human being should not be subject to constant monitoring even when moving in public space. However, the tension between the idea that one should be free from persistent public observation and the Court's Fourth Amendment doctrine is being exposed with the increasing development and governmental deployment of surveillance technologies. For instance, beeper devices, which may have tracked a limited amount of information, often for limited periods of time, bear only an attenuated resemblance to current location data technologies.[198] The formerly state-of-the-art beeper has long since been surpassed by a host of different GPS technologies.[199] However, older cases remain the law in this field, despite the advance of newer surveillance technologies, such as GPS and unmanned aerial surveillance ("UAS"). The resulting advances in surveillance technology may, in fact, be a natural consequence of the Court's jurisprudence. If constitutional doctrine allows the government to collect information through mechanisms that avoid judicial oversight, why would it not pursue those tools and strategies that allow it to exploit the path of least regulatory resistance? Advances in surveillance technology indicate that law enforcement and industry pay attention to constitutional doctrine and respond to the incentives and disincentives created by the Court's Fourth Amendment jurisprudence. The question raised and reserved by the Court in *Knotts*, therefore, may be more relevant now, as the modern state of surveillance technology suggests a purposeful effort to exploit seams in Fourth Amendment doctrine.[200] While answering the question reserved in *Knotts* is empirically problematic, as there is no test from the Court as to what "abuse" might mean, assessments of the state and usage of two novel yet highly advanced surveillance technologies, GPS and UAS, offer a sense of whether surveillance technologies, that can push the boundaries of the "public" versus the "private," should require greater scrutiny.

GLOBAL POSITIONING SYSTEM

The Global Positioning System consists of a constellation of at least 24 satellites that can measure location three dimensionally in terms of latitude, longitude, and altitude.[201] By calculating the rate of change in these

198. United States v. Jones, 132 S. Ct. 945, 964 n.10 (Alito, J., concurring).

199. *See* discussion *infra* Parts IV.A-B.

200. *See supra* Parts III.A-B.

201. *See, e.g.*, Renee McDonald Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 414–15 (2007) (citing DEF. SCI. BD. TASK FORCE,

three dimensions, GPS satellites can also measure speed and direction of movement.[202] Though originally developed for Department of Defense mission requirements, the system was conceptually embraced by civil and commercial users even before the satellite network reached full operational capability.[203] By 1983, President Reagan had announced that it would be made available for civil use as soon as the system was operational.[204] The civil demand for access to GPS technology continued to increase as a result of its successfully demonstrated capabilities in support of military operations in the Persian Gulf in the early 1990s. As demand grew, this led to subsequent policy announcements and action from the Clinton Administration, specifically promising international civil access to GPS for navigational and surveying purposes.[205] The Department of Transportation and other subordinate federal agencies, such as the U.S. Coast Guard, Federal Aviation Administration, and National Oceanic and Atmospheric Administration, coordinate and make available navigational GPS services to private users that are accurate within approximately one to two meters.[206]

In the discussion about GPS and its use in tracking, one commentator has noted that the "tracking" characterization incorrectly implies that access to its positioning capabilities requires active participation by the GPS user.[207] Rather, GPS is a passive technology, meaning that GPS receivers "simply [read] the information continuously transmitted by orbiting satellites."[208] Constantly receiving and reading these satellite signals, an individual GPS device calculates and translates that information in terms of lo-

---

DEP'T OF DEF., *The Future of the Global Positioning System* 4, 25–26 (2005), *available at* http://www.acq.osd.mil/dsb/reports/2005-10-GPS_ Report_Final.pdf); Scott Pace et al., RAND CORP., *The Global Positioning System: Assessing National Policies*, 218, 237 (1995), *available at* http://www.rand.org/content/dam/rand/pubs/monograph_reports/2007/MR614.pdf.

202. Hutchins, *supra* note 201, at 417 (citing Pace et al., *supra* note 201, at 220).

203. Pace et al., *supra* note 201, at 238.

204. *Id.* at 247–48.

205. *Id.* at 250.

206. DEF. SCI. BD. TASK FORCE, *supra* note 201, at 40; Pace et al., *supra* note 201, at 251–55. This is not pure GPS, but rather a system that incorporates differential GPS techniques. *Id.* Pure GPS is information based solely on the direct communication between multiple orbital satellites, usually four, and a ground-based GPS receiver. *Id.* Differential GPS, however, will also include the use of a ground-based, known-point referent receiver so as to improve the accuracy of the information received from civil GPS signals. *Id.* Additionally, differential techniques may also include information from other referent receivers and networks so as to reduce anomalies still further, thereby further enhancing the accuracy of civil GPS. *Id.*

207. *See* Hutchins, *supra* note 201, at 418 (citing Richard B. Langley, *In Simple Terms, How Does GPS Work*, (Feb. 16, 2008), http://gge.unb.ca/Resources/HowDoesGPSWork.html).

208. Hutchins, *supra* note 201, at 418.

cation, speed, and direction.[209] In other words, only that particular GPS device knows its location, unless it possesses some transmission capability that can send data calculated by the receiver to a third party.[210] However, once that transmission capability is in place, the receiver will then passively and persistently feed that location data for monitoring.

This capability has fed a growing use of GPS surveillance by law enforcement and other government actors. Trying to gain a handle on statistics is difficult as agencies are wary about discussing details of operational tactics, techniques, and procedures.[211] For instance, when reporters asked one police department in Ohio about its use of GPS technologies in making several arrests, the department refused to give many details, describing the topic of GPS surveillance as a "very touchy subject."[212] Despite the lack of comprehensive numbers, some individual agency numbers exist which can offer a sense of the burgeoning employment of this technology.[213] For instance, the Justice Department released documents that revealed that the U.S. Attorney's Office for the District of New Jersey had successfully obtained cell site location information ("CSLI") without a warrant supported by probable cause in seventy-nine cases since September 11, 2001.[214] Additionally, these documents revealed that federal agents obtained GPS or similarly precise location data on target cell phones on nineteen occasions since November 2007.[215] Shifting to the state courts, records from one county court in Ohio show that eighteen tracking-device search warrants were issued in 2009. Of course, neither of these examples offers a comprehensive insight into the volume of warrantless GPS surveillance operations. The lack of information is a consequence of law enforcement agencies' predictable reluctance to discuss their internal methods and policies regarding surveillance operations.[216] And even though the Justice Department

209. *See id.* at 417.

210. *Id.* at 418.

211. James Thalji, *GPS Lets Police Follow Suspects' Every Move*, ST. PETERSBURG TIMES, Oct. 20, 2010, at 1A. (discussing the difficulty of obtaining information regarding law enforcement official's usage of GPS technology).

212. John Futty, *GPS Helping Nab Suspects*, COLUMBUS DISPATCH, Feb. 6, 2010, at 1B (questioning a Columbus police department spokesman about how often GPS technology is used in police investigations).

213. *See, e.g.*, Claire Heininger, *ACLU Assails Christie for Cell Phone Invasions Group Likens Warrantless Traces by U.S. Attorneys to Big Brother*, NEWARK STAR-LEDGER, Apr.. 24, 2009, at 15 (referencing Justice Department statistics associated with use of GPS technology).

214. *Id.* at 15 (referencing statistics released by the ACLU relating to the use of tracking devices without first obtaining a warrant).

215. *Id.*

216. *See GPS Lets Police Follow Suspects' Every Move*, *supra* note 211 (explaining how

has publicly expressed its policy "recommend[ing]" collection of GPS or other CSLI pursuant to a warrant, some U.S. Attorney's offices have resisted.[217]

In addition to considering the handful of statistical examples available, individual reports of GPS surveillance used at all levels of law enforcement illustrate a trend-line of widening use. For example, one former police officer described the advantages of using GPS surveillance to track suspected stalkers, noting the unique nature of the crime and the practical difficulties of maintaining undetected visual surveillance of suspects for lengthy periods of time.[218] In another example, police in a small town in Oklahoma have inserted GPS trackers into utility trailers left as bait for would-be thieves.[219] These baited-trailer operations led to three arrests in 2010.[220] In Atlanta, Georgia, police located a suspected bank robber with the assistance of a GPS receiver planted in one of the bags of cash that he stole.[221] And in investigations ranging from that of a serial arsonist in Boston, to a murderer in Central Florida, police have successfully identified and arrested suspects as a result of the information gained by attaching GPS receivers to vehicles and tracking anomalous movements.[222] In a highly publicized example from 2004, police in California placed GPS receivers on vehicles used by Scott Peterson and recorded several suspicious trips he made to a marina not far from where the body of his murdered wife

---

various law enforcement agencies refused to provide details into agency procedure regarding use of GPS devices).

217. Heininger, *supra* note 213 (reporting that the New Jersey State Attorney informed his staff to regard the Justice Department's recommendation relating to search warrants as advisory); Charles Pope, *Wyden Wants a Law as Modern as Your Phone*, THE OREGONIAN, Sept. 5, 2010 (explaining that the Justice Department's recommendation on collecting location data is not strictly enforced and is often ignored).

218. Yvonee Zipp, *Courts Divided on Use of GPS Tracking: Two Recent, Divergent Court Rulings on Warrantless Tracking Suggest New Technologies are Straining Old Privacy Standards*, CHRIS. SCI. MONITOR, May 15, 2009, at 2 (stating that the use of GPS tracking is especially useful in suspected stalking cases).

219. *Father, Son Arrested in "Bait Trailer" Theft*, THE OKLAHOMAN, Aug. 17, 2010, at 14A (reporting that a father and son were arrested for attempting to steal a trailer equipped with a GPS device).

220. *Id.*

221. Alexis Stevens, *Cops Nab Bank Robbers with Help of GPS Device*, ATL. J. CONST., May 19, 2010, at 3B.

222. *GPS Lets Police Follow Suspects' Every Move*, *supra* note 211 (reporting that police used GPS technology to track a murder suspect in Florida); Johnson O'Ryan, *Dorchester Man Held on Arson Charge*, BOST. HERALD, Aug. 11, 2010, at 2 (detailing how a suspected arsonist's vehicle was fitted with a GPS device which led to the suspect's eventual arrest).

later washed ashore.[223] The State of California used this evidence at trial and ultimately prevailed in convicting Peterson of murder.[224]

Driving the increased use of this technology, especially amongst state and local law enforcement agencies, is decreased sensor cost, improved ease of sensor deployment, and enhanced computer capabilities that support processing of raw data. For example, the cost of an external GPS receiver that an investigator can quickly affix to a vehicle is approximately $700 if purchased on the commercial market.[225] The purchase of this receiver also includes access to a secure website that allows an investigator to continuously track the target right from his computer.[226] However, a GPS tracking receiver need not be that expensive and, depending on the product's capabilities, may cost less than $100.[227] While decreased sensor cost may be one element that makes GPS tracking more enticing, there are other potential costs that need to be accounted for, such as the resultant need to manage and exploit greater volumes of raw data. However, as it happens, the proliferation of sensor generated data has also coincided with the decreased cost and enhanced capacity of data storage and processing.[228] This means that any additional costs of managing and processing increased volumes of raw data are not prohibitive, when calculated along with decreased sensor cost, increased manpower cost-savings, and enhanced operational surveillance capacity.

In addition to the needs of traditional domestic law enforcement investigations, GPS tracking is also being used in support of national security investigations. For instance, Yasir Afifi, a twenty-year-old college student living in San Jose, California, recently discovered a GPS receiver attached

223. April Otterberg, Note, *GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment*, 46 B.C. L. REV. 661, 668–69 n. 55 (describing law enforcement official's use of GPS devices to track Scott Peterson 's vehicles); Stacy Finz & Michael Taylor, *Peterson Tracking Device Called Flawed*, S.F. CHRON., Feb. 12, 2004, at A17 (arguing that evidence obtained from the use of GPS technology to track Peterson's vehicles should not be admitted at trial).

224. Otterberg, *supra* note 223, at 669 n.58; Stacy Finz & Michael Taylor , *Groundbreaking Ruling in Peterson Trial; Tracking Evidence Can be Presented*, S.F. CHRON., Feb. 18 2004, at A11 (reporting that the judge presiding over the Laci Peterson murder trial ruled that evidence obtained from GPS was admissible).

225. Susan Taylor Martin, *No Secret: Technology Dominates Gumshoes' Conference*, ST. PETERSBURG TIMES, Mar. 23, 2010, at 1A.

226. *Id.*

227. Roy Furghott, *More Consumers are Letting Insurers Monitor Their Mileage*, N.Y. TIMES, Dec. 26, 2010, at AU2.

228. Byron Acohido, *Yes, You are Being Watched: Big Brother's Got Nothing on Today's Digital Sensors*, USA TODAY, Jan. 26, 2011, at 1B.

to the undercarriage of his car during an oil change.[229] Not knowing what it was at first, Afifi took photos of the receiver and placed them on the internet, hoping that someone could identify it.[230] Not long after that, Afifi received a visit from FBI agents who ordered him to hand over the GPS receiver or else face criminal charges.[231] In another more successful FBI operation, agents used both vehicle mounted GPS as well as cell phone-based GPS information to track Hosam Smadi, a suspected terrorist who planned to detonate explosives in a Dallas office building.[232] In its warrant application for the use of GPS, federal agents justified the employment of GPS technology because of the heightened risk of any physical surveillance operation being detected in the rural setting where Smadi lived.[233]

UNMANNED AERIAL SURVEILLANCE

Domestic law enforcement agencies at all levels are actively exploring and testing UAS programs for operational use. At the municipal and county levels, several agencies currently have active unmanned aerial surveillance ("UAS") acquisition and testing programs, including the Los Angeles County Sheriff's Department ("LASD"), the Miami-Dade Metro Police, the Houston Police Department, and the Sacramento Police Department.[234] At the federal level, the FBI is exploring their domestic use,[235] and the Customs and Border Patrol ("CBP") has had an operational Predator drone program on the U.S.-Mexico border since 2005.[236] As recently as September 2010, CBP deployed yet another Predator in the vicinity of the Texas international border.[237] Despite the significantly dimin-

229. Bob Egelko, *Man Sues FBI Over GPS Surveillance*, S.F. CHRON., Mar. 3, 2011, at C3; Paul Elias, *Use of GPS for Surveillance Spurs Privacy Debate; One Judge Describes the Practice as Orwellian, but some Disagree*, THE STAR-LEDGER, Oct. 17, 2010, at 7; *GPS Lets Police Follow Suspects' Every Move*, *supra* note 211.

230. Egelko, *supra* note 229; Elias, *supra* note 229.

231. Egelko, *supra* note 229; Elias, *supra* note 229.

232. Jason Trahan, *Officials Scour Digital Files of Terror Suspect*, DALLAS MORNING NEWS, Jan. 10, 2010, at B1 [hereinafter Trahan, *Officials Scour*]; Jason Trahan, *FBI Says Teen Had Firearms; Affidavits also Note Difficulty in Tailing Someone in Small Town*, DALLAS MORNING NEWS, Oct. 7, 2009, at B1 [hereinafter Trahan, *Affidavits*].

233. *FBI Says Teen Had Firearms; Affidavits also Note Difficulty in Tailing Someone in Small Town*, *supra* note 232.

234. Travis Dunlap, Comment, *We've Got Our Eyes on You: When Surveillance by Unmanned Aircraft Systems Constitutes a Fourth Amendment Search*, 51 S. TEX. L. REV. 173, 180–81 (2009).

235. *Robocop May Join in Miami Vice Fight*, THE AUSTRALIAN, Apr. 1, 2008, at 35.

236. Dunlap, *supra* note 234, at 180.

237. Lynn Brezosky, *Border-Patrolling Drones to Call Texas Base Home; Crafts Can Spot*

ished cost of acquiring and operating UAS platforms, their field deployment has been restrained because of FAA regulations limiting their presence in the national air space.[238] However, that will likely change soon, as the FAA intends to announce new, more permissive regulatory guidance in this area.[239] In fact, the 2012 FAA Reauthorization Act mandates that the agency develop regulations for the operation of private commercial drones by 2015 and for police and emergency responders by the end of 2012.[240]

In recent years, with wars in Iraq and Afghanistan, UAS has come to the forefront of national attention. These aerial vehicles, used with remarkable success in both theaters, have been employed in missions ranging from aerial reconnaissance to strike missions in Pakistan.[241] While there are many makes and models, clearly the one most well known is the Predator. Though most notable for its use in defense and intelligence work overseas, the MQ-9 Predator B is no longer an expatriate and is quickly finding an operational home in the United States.[242] Weighing in at nearly five tons, measuring thirty-nine feet in length, and costing nearly $4.3 million to purchase,[243] this is certainly no model airplane. And, according to former CBP Commissioner Alan Bersin, the results speak for themselves. Since their deployment debut on U.S. borders, the Predator is credited with leading to the interdiction of more than 39,000 pounds of illegal drugs and the capture of more than 7,000 illegal border crossers.[244] To Bersin, their effectiveness is clear, as he declares that they are a "powerful force multiplier."[245] Currently, CBP operates at least five Predators between both the northern and

---

Drug Smugglers, Illegal Crossings, HOUS. CHRON., Sept. 9, 2010, at B3.

238. Dan Glaister, *LA Sheriff's Pilotless Spy Plane Grounded*, THE GUARDIAN, June 23, 2006, at 16.

239. Sandra I. Erwin, *Non-Military Market for Unpiloted Aircraft Will Remain Sluggish*, NATIONAL DEFENSE (Aug. 1, 2010), http://www.nationaldefensemagazine.org/archive/2010/August/Pages/NonMilitaryMarketforUnpilotedAircraftWillRemainSluggish.aspx.

240. Patrick Hruby, *Out of 'Hobby' Class, Drones Lifting Off For Personal, Commercial Use*, WASH. TIMES (Mar. 14, 2012); Shaun Waterman, *Drones over U.S. Get OK by Congress*, WASH. TIMES (Feb. 7, 2012), http://www.washingtontimes.com/news/2012/feb/7/coming-to-a-sky-near-you/.

241. Mike M. Ahlers, *FAA Urges Caution in Expanding Use of Unmanned Aircraft*, CNN (July 15, 2010), http://articles.cnn.com/2010-07-15/us/unmanned.aircraft_1_unmanned-aircraft-accident-rate-uavs?_s=PM:US.; Siobhan Gorman, *Drones get Ready to Fly Into Daily Life*, WALL ST. J., Nov. 3, 2010, at A16.

242. Brezosky, *supra* note 237.

243. *Id.*; Laura B. Martinez, *Drone to be in Service by Sept. 1*, BROWNSVILLE HERALD (July 15, 2010), http://www. brownsvilleherald.com/articles/cuellar-114415-hearing-used.html.

244. Brezosky, *supra* note 237.

245. *Id.*

southern U.S. borders.[246] Most recently, with a newly granted authorization from the FAA, the CBP augmented its southern border operations by adding a permanently based Predator in Texas to its fleet.[247] While only five CBP Predators are currently deployed in support of border operations, lawmakers envision a substantial increase.[248] For instance, Representative Henry Cuellar (D-Laredo) intends to push for a total of twenty-four Predators to cover America's northern and southern international borders.[249] On its way toward that goal, CBP estimated that it would have at least seven in operation by the end of 2010.[250]

However, CBP is not the sole law enforcement organization seeking to put into operation this formerly military-exclusive technology. In fact, a wide host of local law enforcement agencies have made tangible efforts to purchase and evaluate the feasibility of adding UAS platforms to their operational schemes.[251] Of course, this seems implausible in light of the cost of the Predator. In addition to its hefty acquisition price, which would cost at least twice as much as the average manned helicopter used in general civil aviation,[252] the annual operational cost commitment for a predator is between seven and eight million dollars.[253] In a fiscal environment where municipal police departments are already dumping manned aviation programs because of cost,[254] how can such an expensive technology be anywhere on a local police chief's priority list?

The answer to that question has come in the form of a newly burgeoning UAS aviation industry. Even though defense acquisitions have primarily revolved around larger platforms, such as General Atomics' Predator and Northrop Grumman's Global Hawk, the industry-wide increase in annual sales[255] represents a broadening of the market, where companies are now marketing a new generation of less costly UAS platforms to potential

246. Martinez, *supra* note 243.

247. *Id.*

248. Brezosky, *supra* note 237; Martinez, *supra* note 243.

249. Brezosky, *supra* note 237 (discussing how lawmakers intend on increasing surveillance).

250. *Id.*; Martinez, *supra* note 243.

251. John Lantigua, *Miami-Dade Hoping to Use Unmanned Aircraft to Fight Crime*, PALM BEACH POST, Mar. 27, 2008, at A1; David Slade, *Robo-copters Might Fly into City; Charleston Police Hope to Buy Drones*, THE POST AND COURIER, Feb. 17, 2008, at B1; Daniel B. Wood, *It's a Kite. It's a Model Airplane. It's . . . the Sheriff*, CHRIS. SCI. MONITOR, July 11, 2006, at 1.

252. Martinez, *supra* note 243; Wood, *supra* note 251.

253. Martinez, *supra* note 243.

254. Slade, *supra* note 251.

255. Max Jarman, *Pilotless Aircraft Tested in Arizona*, ARIZ. REPUBLIC, May 18, 2008, at 1 (highlighting the flourishing aviation industry).

clients, who may not need the robust capabilities of the highest echelon platforms operated in the defense and national intelligence sectors. Amongst the most promising in this new class is the Honeywell Micro Air Vehicle ("MAV"). Costing $250,000 to acquire, its fiscal feasibility only begins with its purchase price. According to one estimate, operating a manned helicopter can cost up to $1,200 per hour, and that is not including the cost of having human assets, typically three people, operate and provide ground control for the helicopter during flight.[256] And, even though the MAV may not possess the endurance[257] or range and speed[258] that a Predator would, it can travel as fast as fifty knots and operate at an altitude of up to 10,500 feet.[259] Similar small UAVs being tested by the Charleston, South Carolina Police Department ("CPD") and the LASD would offer thermal imaging optics[260] and flight endurance of up to seventy-five minutes. Additionally, because of their small size, they can be stored in the trunk of a vehicle, driven to any location, and launched in the field. For instance, the SkySeer platform, tested by LASD, is so small and quiet that it is no louder than the sound of a buzzing mosquito at twenty feet away and is audibly undetectable beyond that distance.[261]

Even though police departments, when asked about potential surveillance capabilities of UAS, generally respond that they have no interest in peering into the windows of citizens,[262] that does not mean that UAS surveillance capabilities will not eventually be exploited in situations that begin to trigger privacy concerns. For instance, the chief of the CPD acknowledged an interest in using this technology to provide aerial overwatch of large crowds and to use them in order to track suspects, including at night with the assistance of thermal optics.[263] In fact, proving the operational feasibility of such a use, police in England are already employing small UAVs outfitted with thermal imagery technology to silently track suspects from the sky.[264] But even if law enforcement in the U.S. never in-

256. Wood, *supra* note 251 (noting the ability to acquire an aircraft is easier than ever).
257. Brezosky, *supra* note 237.
258. Wood, *supra* note 251.
259. Lantigua, *supra* note 251.
260. Slade, *supra* note 251 (discussing new features available in aircrafts).
261. Wood, *supra* note 251 (examining the effects of quiet aircraft capability on surveillance).
262. Lantigua, *supra* note 251.
263. Slade, *supra* note 251.
264. *Celebs Beware! New Pandora's Box of 'Personal' Drones That Could Stalk Anyone from Brangelina to Your Own Child*, DAILY MAIL (Nov. 8, 2010) [hereinafter *Celebs Beware*], http://www.dailymail.co.uk/sciencetech/article-1327343/Personal-recreation-drones-developed.html.

tend to employ them as a surveillance tool, it is clear that private actors, benefiting from industry-wide reduced cost of such technology,[265] may certainly intend to use it for that very purpose. For instance, private investigators hired to detect spousal infidelity or tabloid journalists interested in getting above the walls of the rich and famous will clearly have every incentive to employ this technology for the sole purpose of invading individual privacy.[266] With all of the new potential customers, both government and private, apparently lining up to learn more about what the latest generation of UAS can offer them, it is no wonder that industry experts are now just "waiting for the civilian market to erupt."[267]

ATTEMPTING TO DEFINE A RIGHT TO PRIVACY IN PUBLIC SPACE

Increased employment of surveillance technologies, such as GPS and UAS, will cause continued constriction of the boundaries that separate the places where individuals may seek refuge from observation. Even though these technologies may not, in light of *Kyllo*, bootstrap themselves into the home, or other places where an expectation of privacy may attach, they will continue to erode the perceived solitude enjoyed by persons in places that, though outside the home, possess attributes consistent with a sense of private autonomy.[268] Examples might include: public parks, streets, or green spaces in a neighborhood; parking lots adjacent to doctors' or attorneys' offices; or sidewalks or roads traveled upon when a person is attending to errands. While these activities and places may have always received little protection as a constitutional matter, it cannot be said that human beings did not depend on some sense of individual autonomy or anonymity while living in these public spaces.[269] Though outside the express protection of the Court's Fourth Amendment doctrine, should not human dignity require that some activities, though technically public in nature, be performed with an assumption that they are not amenable to constant observation, surveillance, or measurement? In the specific context of GPS surveillance, the

265. *See, e.g.*, BROOKSTONE, http://www.brookstone.com/ar-drone-quadricopter.html?his=2%7E46337%7E2%7Eroot_category%40kwd%7Ehelicopter&bkiid=searchResults|C4CategoryProdList1FDT|9319170 (last viewed Apr. 20, 2011) (marketing a drone, the "Parrot A.R. Drone Quadricopter," which retails at $299.99).

266. *Celebs Beware*, *supra* note 264; Gorman, *supra* note 241.

267. Jarman, *supra* note 255.

268. *See* WESTIN, *supra* note 197, at 31.

269. *See id.*

D.C. Circuit Court of Appeals attempted to answer this broader question—does the Fourth Amendment, under the conditions of modern surveillance technology, expand to include a constitutionally protected right to privacy in public spaces and, if so, under what circumstances should such a protection attach?

UNITED STATES V. MAYNARD

Appellate courts in the last few years have been confronted with the modern problem of persistent surveillance in publicly accessible spaces. This broader question has manifested itself in the specific technological context of GPS tracking. This specific form of remote surveillance has advanced to a point where the questions deferred by cases such as *Knotts* and *Riley* seem far less speculative.[270] This has resulted in a fresh strain of litigation, ultimately asking whether continuous and uninterrupted monitoring of a person's movements in public without judicial review would strain the bounds of *Knotts* and the doctrinal distinction between inside-as-private and outside-as-public.[271] While the courts that have heard these cases have applied *Knotts* in a doctrinally straightforward fashion, finding that such monitoring does not constitute a search, and therefore would not require a warrant,[272] the D.C. Circuit in *United States v. Maynard*[273] came to a different conclusion by means of an analytical approach that does not strictly adhere to inside-outside distinction in discerning the recognition of privacy.

In *Maynard*, several co-conspirators, including defendant Antoine Jones, were suspected of possession and distribution of cocaine.[274] As a part of this investigation, law enforcement installed a GPS tracking device on Jones's Jeep without a warrant.[275] Over the course of four weeks, the device provided law enforcement real-time, twenty-four hour tracking of Jones's vehicle and its position.[276] On appeal, Jones questioned whether law enforcement had violated the Fourth Amendment by tracking him with

270. *See* United States v. Knotts, 460 U.S. 276, 283–84 (1983).

271. *See supra* Part III.C.

272. *See* United States v. Marquez, 605 F.3d 604 (8th Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010); United States v. Garcia, 474 F.3d 994 (7th Cir. 2007).

273. 615 F.3d 544 (D.C. Cir. 2010).

274. *Id.* at 549.

275. *Id.* at 555. Though there was some debate as to this point during the course of litigation, the government eventually conceded, as the GPS was not installed in accordance with the conditions of the warrant that had previously been obtained. *Id.* at 567 n.1.

276. *Id.* at 555.

a GPS device for several weeks without a warrant.[277]

Knotts and the Question of "Dragnet" Surveillance

In its treatment of Jones's objection, the D.C. Circuit broke down the analysis into several separate questions in order to determine whether the prolonged use of GPS surveillance was a search. First, the court confronted whether *Knotts* squarely controlled.[278] If the court viewed Jones's case as merely one of quantitatively greater surveillance, without slipping into the realm of being qualitatively different surveillance, then a straightforward application of *Knotts* would seemingly foreclose objection to any persistent use of GPS surveillance.[279]

In addressing this threshold problem, Judge Douglas Ginsburg, writing for the court, found that *Knotts* did not control under these facts.[280] Specifically, the court noted that *Knotts* emphasized the limited use of the device to a single trip, and that its use was supplemental to visual surveillance performed by law enforcement.[281] The court also read *Knotts* as having explicitly reserved the question of warrantless, persistent surveillance.[282] The Government argued that *Knotts* only excluded the question of mass, "dragnet" surveillance of members of the public for whom there was no suspicion of any criminal conduct.[283] Judge Ginsburg, however, observed that the Supreme Court addressed this question in response to the objection raised by the defendant in *Knotts*, which specifically proffered the problem of "twenty-four hour surveillance," not suspicionless surveillance.[284] Therefore, what the Supreme Court responded to and reserved was just that specific argument—the constitutional appropriateness of warrantless, persistent surveillance, regardless of whether it targeted the public as a whole or those particularly suspected of criminal activity.[285]

---

277. *Id.*

278. *Id.* at 556.

279. *Maynard*, 615 F.3d at 556.

280. *Id.* at 558 ("As we have explained, in *Knotts* the Court actually reserved the issue of prolonged surveillance. That issue is squarely presented in this case.").

281. *Id.* at 556 (citing United States v. Knotts, 460 U.S. 276, 283–85 (1983)).

282. *Id.* at 556; *Knotts*, 460 U.S. at 283–84 ("[I]f 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.").

283. *Maynard*, 615 F.3d at 556.

284. *Id.*; *see Knotts*, 460 U.S. at 283.

285. *Maynard*, 615 F.3d at 556–57 (explaining three circuit courts have come down on the opposite side of this issue, finding, or at least assuming, that the issue preserved by *Knotts* was the one of wholesale or mass surveillance); *see* United States v. Marquez, 605 F.3d 604, 610 (8th

Having isolated the issue reserved in *Knotts*, Judge Ginsburg determined that *Knotts* merely stood for the proposition that individuals traveling in an automobile on a public thoroughfare have no reasonable expectation of privacy in their "movements from one place to another, not that such a person has no reasonable expectation of privacy in his movements whatsoever, world without end . . . ."[286] Establishing this narrowed view of *Knotts*, the court contrasted the facts in *Maynard*, concluding that the issue of persistent surveillance raised in this case is the precise problem contemplated and reserved by the Supreme Court in *Knotts*.[287] The importance of this conclusion cannot be underestimated, because having shed the controlling burden of *Knotts*, the *Maynard* court could permit itself to engage in the fuller normative discussion of the Fourth Amendment's boundaries that leads to the formulation of the "mosaic theory."

Actual Exposure

Analytically free to assess the case from doctrinal origins, the court looked to *Katz* and asked whether the defendant had an expectation of privacy that society was prepared to recognize as reasonable.[288] To determine the presence of such a privacy expectation, the court observed that "[w]hether an expectation of privacy is reasonable depends in large part upon whether that expectation relates to information that has been 'expose[d] to the public.'"[289] The issue then was to determine what it meant to "expose" something to the public under these circumstances. The *Maynard* court proceeded by splitting this problem into two sub-questions: first, whether a person's conduct had been "actually" exposed to the public;[290]

Cir. 2010) ("[W]hen police have reasonable suspicion that a particular vehicle is transporting drug, a warrant is not required when, while the vehicle is parked in a public place, they install a non-invasive GPS tracking devise on it for a reasonable period of time."); United States v. Pineda-Moreno, 591 F.3d 1212, 1217 (9th Cir. 2010) ("[T]he police did not conduct an impermissible search of Pineda-Moreno's car by monitoring its location with mobile tracking devises."); United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007) ("GPS tracking is on the same side of the divide with the surveillance cameras and the satellite imaging, and if what they do is not searching in Fourth Amendment terms, neither is GPS tracking.").

286. *Maynard*, 615 F.3d at 557; *see Knotts*, 460 U.S. at 281 ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

287. *Maynard*, 615 F.3d at 558.

288. *Id.*

289. *Id.*; *see* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject Fourth Amendment protection.").

290. *Maynard*, 615 F.3d at 559.

and second, whether that same conduct had been "constructively" exposed.[291]

In its discussion of how to find "actual" exposure, the court quickly identified and rejected the government's position.[292] The government asserted that the defendant's movements were actually exposed to the public, because law enforcement "could have followed" the defendant's movements anywhere and everywhere on the public roads for the month that it tracked him remotely by GPS.[293] This can be thought of as a rule of pure potentiality—so long as law enforcement had the potential to visually surveil the suspect in person, then his conduct was "actually exposed" to the public, thereby removing any Fourth Amendment protection.

In response, the court found that any test focusing on mere physical or lawful ability to conduct surveillance misses the point of *Katz*. Rather, the question of whether something is publicly exposed turns on "what a reasonable person [would] expect another [person] might actually do."[294] In support of this proposition, Judge Ginsburg cited to several cases, including *Bond v. United States*.[295] In *Bond*, the defendant was a passenger on a cross-country bus and placed a carry-on bag in a storage area above his seat.[296] During a stop, law enforcement boarded the bus and walked up and down the bus aisle, feeling and squeezing luggage in order to find drugs.[297] The effort succeeded in the sense that agents discovered a brick of methamphetamine in the defendant's bag.[298] Though factually dissimilar from *Maynard*, this case, according to Judge Ginsburg, raised the same fundamental problem—whether to recognize a reasonable expectation of privacy in conduct placed in the public sphere. From the Supreme Court's perspective, the problem of reasonable privacy expectations in *Bond* did not turn on mere potentiality, *i.e.*, whether fellow passengers or bus line employees feasibly could access and manipulate a person's luggage, "but rather upon what a reasonable bus passenger expect[ed] others . . . might actually do."[299] Applying this principle, the Supreme Court concluded that

291. *Id.* at 560–61.
292. *Id.* at 559.
293. *Id.*
294. *Id.*
295. *Id.*; Bond v. United States, 529 U.S. 334, 339 (2000) (holding "the agent's physical manipulation of the petitioner's bag violated the Fourth Amendment.").
296. *Bond*, 529 U.S. at 335; *see Maynard*, 615 F.3d 559.
297. *Bond*, 529 U.S. at 335; *see Maynard*, 615 F.3d at 559–60.
298. *Maynard*, 615 F.3d at 560.
299. *Id.*

people do not expect to have their baggage routinely manipulated in an exploratory manner, but instead have a reasonable expectation to be free from such warrantless investigation conducted by members of the public, as well as government agents.

Employing the logic of "reasonable likelihood" from *Bond*, Judge Ginsburg and the majority determined that the defendant's movements were not actually exposed to public view. While discrete acts may have been exposed to the public, the whole of the defendant's movements over the course of one month were not. Indeed, "the likelihood a stranger would observe all those movements [was] not just remote [but] essentially nil."[300] So unlike *Knotts*, where law enforcement sought to identify a target's single movement (something easily observed by a member of the public), law enforcement here sought to know an entire private routine. Without GPS technology, this could only be accomplished through constant visual surveillance, "dogging [the] prey" on a daily basis so as to learn the entire architecture of a person's activities.[301] For the court, because such conduct and aggregate information is so unlikely to be acquired by the general public, it cannot be characterized as having been "actually exposed" to the public's view.[302]

Constructive Exposure

Having concluded that the defendant's movements were not "actually exposed" to the public, the *Maynard* court then introduced a different articulation of the problem, asking whether his movements were "constructively exposed" to the public.[303] Though a fine distinction from the concept of "actual exposure," when the court asked whether the defendant's movements over the course of a month were "constructively exposed," it seems to have been questioning whether the defendant's movements should be categorically deemed to have been exposed for the simple reason that every movement tracked in this case occurred in the public sphere.[304] The court found that the defendant's movements were not "constructively exposed," because the month-long entirety of his movements, though available for public view, conveyed qualitatively different information when coalesced

300. *Id.*
301. *Id.*
302. *Id.* at 562.
303. *Id.* at 560–61.
304. *Maynard*, 615 F.3d at 560–61.

and analyzed as a whole.[305] The court concluded that the aggregation of a person's travels over a month's course was more revealing and, as such, something qualitatively different than its individual parts.[306] In essence, the government had constructed a detailed "mosaic" of the defendant's life by collecting a large volume of travel-oriented information about him.[307]

Conceptually, the "mosaic theory" is a recognition of how facts are infused with meaning and, therefore, value. It acknowledges that highly discrete slices of information often have little import, but that an observer with a comprehensive factual perspective can often discern significance from seemingly trivial individual items.[308] In developing this general concept for its novel application to the Fourth Amendment, the *Maynard* court looked to what it considered analogous cases dealing with the Privacy Act[309] and the Freedom of Information Action Act ("FOIA").[310]

For instance, the *Maynard* court cited to *J. Roderick MacArthur Foundation v. FBI*, a case in which a group sought to have the FBI purge all files and other records that pertained to its "associational activities and to refrain from maintaining such records in the future."[311] The group claimed there was no longer any law enforcement necessity to maintain this information; therefore, the FBI's continued maintenance of the file violated the Privacy Act.[312] Concurring with the government's position, the court ruled the FBI must be able to maintain information, even from closed investigations.[313] Seemingly innocuous information can often times play an important role in future investigations in ways that are difficult to anticipate.[314] Without maintenance of a wide spectrum of lawfully collected information, the government would lose an important investigatory technique, which is the ability to create and draw meaningful inferences from a "mosaic" of individually less meaningful items.[315] For additional support, the *Maynard* court also cited to *United States v. Sims*, a case where the Su-

305. *See id.* at 561–62.

306. *Id.* at 562 ("These types of information can each reveal more about a person than does any individual trip viewed in isolation.").

307. *Id.*

308. *Id.* (citing CIA v. Sims, 471 U.S. 159, 178 (1985)); *see* J. Roderick MacArthur Found. v. F.B.I. *(JRM Found.)*, 102 F.3d 600, 604 (D.C. Cir. 1996)).

309. 5 U.S.C. § 552a (2010).

310. 5 U.S.C. § 552 (2010).

311. *Maynard*, 615 F.3d at 562; *JRM Found.*, 102 F.3d at 601.

312. *JRM Found.*, 102 F.3d at 602.

313. *Id.* at 604.

314. *Id.*

315. *Id.* (citing *In re* United States, 872 F.2d 472, 475 (D.C. Cir. 1989)).

preme Court rejected a FOIA request for the names of persons involved in a secret CIA program.[316] In that case, the Court discussed with approval the intelligence community's analytical methods in gathering large volumes of information from open sources in order to detect broader insights or trends.[317]

From the *Maynard* court's perspective, these cases function as a sort of government admission that "mosaics" are qualitatively different and more revealing than discrete items of information. However, *Sims* and *MacArthur Foundation* can only stand for that narrow conceptual proposition—that informational "mosaics" offer qualitatively different meaning than the individual facts that comprise the whole. If the court was depending upon these cases in support of its "mosaic theory" approach, only such a narrow view of the cases would offer any support. Read more broadly, however, these cases actually affirm the government's interest in collecting wide swathes of information, especially from sources that are open and available in the public sphere.[318] While the Court in *Sims*, for instance, specifically approved of intelligence collection from open media outlets,[319] it could have just as easily included a discussion on the conceptual analogue of surveillance of public spaces. Even though these cases buttress the most basic conceptual propositions underlying the "mosaic theory," they do so only in a context that tends to affirm government information collection and retention. In light of these cases, the *Maynard* court still had to find some precedential support for the proposition that publicly available information in the aggregate translates into something which society would recognize as uniquely private when collected by the government. The *Maynard* court cited to two cases in an attempt to bridge this gap.

First, the court found support for the principle that an individual possesses a privacy interest in aggregated information, even though its component parts are available as a matter of public record, in the case of *United States Department of Justice v. Reporters Committee for Freedom of Press*.[320] There, the Supreme Court heard a challenge to the FBI's invocation of the privacy exception to a FOIA request.[321] The request sought the

316. *Maynard*, 615 F.3d at 562; CIA v. Sims, 471 U.S. 159, 178 (1985).

317. *Sims*, 471 U.S. at 167–73.

318. *See id.* at 171–72; J. Roderick MacArthur Found. v. F.B.I. (*JRM Found.*), 102 F.3d 600, 604 (D.C. Cir. 1996).

319. *Sims*, 471 U.S. at 171–72.

320. *Maynard*, 615 F.3d at 561 (citing U.S. Dep't. of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749 (1989)).

321. *Reporters Comm.*, 489 U.S. at 751.

criminal records of several persons allegedly connected to a Congressman who had been implicated in a government contracting corruption investigation.[322] In finding for the Government, the Court held that an individual possesses a privacy interest in the aggregated "rap sheet" created by the FBI, despite the fact that the information contained therein might be publicly available in its individual parts.[323] According to the Court, the privacy interest in a compilation document is altered in favor of the individual because of the "vast difference between the public records that might be found after a diligent search of courthouse files . . . and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[324] But for the assistance of an FBI computer database, the requesting party could not reasonably expect to succeed in the difficult task of manually collecting each and every criminal record that would comprise a "rap sheet."[325] Therefore, the subjects of this request possessed a privacy interest in the qualitatively different "whole" as something that was distinct from the publicly available "bits of information" of which it was comprised.[326] Also, the Court clearly suggested that this privacy interest is heightened as a result of advances in information technology, which allow for easier accumulation and storage of information "that would otherwise have surely been forgotten . . . ."[327] Ultimately, the Court, citing to the "common law"[328] and various statutes, including FOIA and the Privacy Act, concluded that government disclosure of a compiled record of information, such as a complete criminal history in this case, constitutes an unwarranted invasion of personal privacy.[329]

Though *Reporters Committee* offered an affirmation of the concept that an individual can maintain a privacy interest in an informational composite, it still had clear limitations as controlling authority in support of the *Maynard* court's Fourth Amendment "mosaic theory." Notably, the Court did not announce a constitutional or, more particularly, a Fourth Amendment principle. Aside from an ambiguous reference to the "common law,"[330] the case was, as a jurisprudential matter, an assessment of a statu-

322. *Id.* at 757.
323. *Id.* at 780.
324. *Id.* at 764.
325. *See id.* at 764, 770–71 (quoting Rehnquist, *supra* note 1, at 13).
326. *Id.* at 765.
327. *Reporters Comm.*, 489 U.S. at 770–71 (quoting Rehnquist, *supra* note 2, at 13).
328. *Id.* at 763.
329. *Id.* at 780.
330. *Id.* at 763.

tory right gleaned from FOIA and the Privacy Act.[331] Moreover, *Reporters Committee* only affirmed a privacy interest in aggregate information as against private parties. Never once did the Court imply that the government could not maintain and use *ad infinitum* lawfully collected records against individuals.[332] Quite to the contrary, the Court assumed that one of the clearly appropriate purposes of collecting and using compiled information is for law enforcement purposes.[333] While this case provided some additional conceptual support for a broad sense of privacy in facts that are available in the public sphere, it offered no assistance when applied to the specific policy interests of the Fourth Amendment.

Despite the dissimilarities between these cases and the facts in *Maynard*, the D.C. Circuit ultimately found defendant Jones's privacy interest as one society was prepared to recognize as reasonable.[334] Notwithstanding all of the movements tracked were in the public sphere, the court found that the "use of the GPS device to monitor those movements defeated that reasonable expectation . . . [by] reveal[ing] an intimate picture of the subject's life that he expects no one to have . . . ."[335] The court found no reasonable person would "expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain 'disconnected and anonymous.'"[336] Despite the Govern-

331. *See id.* at 751 ("The question presented by this case is whether the disclosure of the contents of such a file to a third party 'could reasonably be expected to constitute an unwarranted invasion of personal privacy' within the meaning of the [FOIA].") (citation omitted).

332. *See id.* at 780.

> Accordingly, we hold as a categorical matter that a third party's request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen's privacy, and that when the request seeks no "official information" about a Government agency, but merely records that the Government happens to be storing, the invasion of privacy is "unwarranted."

Id.

333. *Reporters Comm.*, 489 U.S. at 764–65.

> This conclusion is supported by the web of federal statutory and regulatory provisions that limits the disclosure of rap-sheet information. That is, Congress has authorized rap-sheet dissemination to banks, local licensing officials, the securities industry, the nuclear-power industry, and other law enforcement agencies. Further, the FBI has permitted such disclosure to the subject of the rap sheet and, more generally, to assist in the apprehension of wanted persons or fugitives. Finally, the FBI's exchange of rap-sheet information "is subject to cancellation if dissemination is made outside the receiving departments or related agencies."

Id. (citations omitted).

334. *Maynard*, 615 at 563.

335. *Id.*

336. *Id.* (citing Nader v. Gen. Motors Corp., 25 N.Y.2d 560, 572 (1970) (Breitel, J., concurring)).

ment's contention that the defendant lacked a reasonable privacy expectation as soon as he left his home and entered his vehicle, the court found no such categorical rule appropriate in this case. Citing *Katz*, the court asserted that even publicly accessible space can potentially accommodate constitutionally protected expectations of privacy, because one's zone of privacy is not fixed to the home, but rather bounded only by "the individual's own reasonable expectations of privacy."[337] Included in the defendant's zone of privacy is the uniquely intimate portrait of his life that, but for the GPS monitoring employed in this case, would otherwise be unavailable to anyone except his closest personal confidants.[338] The *Maynard* court found only one conclusion appropriate in this case—that society recognizes as reasonable the defendant's expectation to have his continuous public movements remain unmonitored.[339]

"Mosaic Theory" and Its Implications for Surveillance Technologies

Finally, the *Maynard* court addressed whether its ruling will necessarily impact other forms of visual surveillance.[340] The court addressed this in response to the government concern that finding an expectation of privacy in public spaces would logically "prohibit even visual surveillance of persons or vehicles . . . exposed to public view," an outcome which it asserted was clearly contrary to law.[341] The court disagreed, however, believing that its newly announced "mosaic theory" approach would have little effect on traditional, in-person visual surveillance.[342] For the court, the critical difference was the use of technology in monitoring activities in the public sphere. As a practical matter, GPS surveillance poses a problem that traditional human surveillance could almost never create.[343] Human surveillance, because of its labor and cost-intensiveness, has a self-regulating aspect that prevents it from lasting longer than what is operationally necessary or feasible.[344] Removing the human element from surveillance, therefore, also removes much of the marginal and fixed costs that persistent human surveillance would necessarily carry. Because GPS and similar technologies make persistent or otherwise impractical surveillance strate-

337. *Maynard*, 615 F.3d at 563 (quoting *Reporters Comm.*, 593 F.2d 1030 at 1042–43).
338. *Id.*
339. *Id.*
340. *Id.* at 565–66.
341. *Id.* at 565.
342. *Id.* at 565–66.
343. *Maynard*, 615 F.3d at 565.
344. *Id.*

gies more cost effective and efficient, they pose a significantly different and "unknown type of intrusion into . . . ordinarily and hitherto private enclave[s]."[345]

From this perspective, the court reminded the government that the means of surveillance do matter in Fourth Amendment analysis.[346] As an example, the court noted that conversations may be recorded through the use of an informant but not by wire tap.[347] This example reflects the principle that reasonable expectations to control one's own information, words in the example, shift depending on the means used to capture that information. Similarly, just because one's movements in the public sphere can be observed and tracked, it does not necessarily follow that this can be done by any technological method available.

UNITED STATES V. JONES AND THE FUTURE OF THE "MOSAIC THEORY"

In the re-styled *Jones* case, the Supreme Court reviewed *Maynard* and, in a somewhat surprising result, unanimously affirmed the D.C. Circuit's decision.[348] Though remarkable for its unanimity of result, the real significance lies in the Court's lack of unanimity as to rationale.[349] The *Jones* case, though comprised of three opinions, is not a plurality decision. Rather, it has a majority holding premised upon a narrow rationale, coupled with two concurring opinions.[350] To be clear, none of the opinions in the *Jones* case ever once used the word "mosaic." However, the reasoning contained in both of the concurring opinions closely tracks the substantive elements of the lower court's rationale in *Maynard*.[351] Though not endorsing Judge Ginsburg's "mosaic theory" expressly by name, the *Jones* concurring opinions can only be read as strong evidence of support by a majority of the Court for the *Maynard* "mosaic" rationale.[352]

---

345. *Id.*

346. *Id.* at 566 (quoting Kyllo v. United States, 533 U.S. 27, 35 n.2 (2001)).

347. *Id.* (citing Katz v. United States, 389 U.S. 347, 353 (1967); Lopez v. United States, 373 U.S. 427, 429 (1963)).

348. *See* Lyle Denniston, *Opinion Recap: Tight Limit on Police GPS Use (FINAL UPDATE)*, SCOTUSBLOG (Jan. 23, 2012, 11:58 AM), http://www.scotusblog.com/2012/01/opinion-recap-tight-limit-on-police-gps-use/.

349. *Id.*; *see also* Tom Goldstein, *Why Jones is Still Less of a Pro-Privacy Decision than Most Thought (Conclusion Slightly Revised Jan. 31)*, SCOTUSBLOG (Jan. 30, 2012, 10:53 AM), http://www.scotusblog.com/2012/01/why-jones-is-still-less-of-a-pro-privacy-decision-than-most-thought/.

350. *See* Denniston, *supra* note 348.

351. *What's the Status of the Mosaic Theory After Jones?*, *supra* note 26.

352. *See id.*

Interesting in its own right, the Court's opinion, written by Justice Scalia and joined by Chief Justice Roberts and Justices Kennedy, Thomas, and Sotomayor, reinvigorates the entire line of pre-*Katz* trespass jurisprudence.[353] Writing for the Court, Justice Scalia finds that physical intrusion upon private property—a vehicle in this case—for the purpose of obtaining information constitutes a Fourth Amendment search.[354] More surprisingly, Justice Scalia pointedly rejects *Katz* as applicable at all in this case.[355] While he recognizes *Katz* as one authoritative standard in assessing the threshold question of whether a search has occurred, he believes that *Katz* never supplanted the basic trespass test from *Oldman*.[356] Rather, "the *Katz* reasonable-expectation-of-privacy-test has been *added to*, not *substituted for*, the common-law trespassory test."[357] In a case where the government intrudes upon a constitutionally enumerated area—an "effect" in the case of *Jones*—the Court has no need to turn to *Katz*.[358] With this analytical move, Justice Scalia and the majority successfully distinguished *Knotts* and *Karo* from *Jones*.[359] In those cases, government agents had not trespassed upon suspects' property, because the suspects had willingly accepted the containers as they came, tracking beepers and all.[360] According to Justice Scalia, because no technical trespass took place in either *Knotts* or *Karo*, the Court had to apply the non-trespassory *Katz* formulation in the present case.[361] In Justice Scalia's estimation, the use of *Katz*'s broader formulation was, therefore, unnecessary in *Jones* because of this categorical distinction. The Fourth Amendment has long been understood, according to Justice Scalia, to protect against government trespass upon certain enumerated areas for the purpose of collecting evidence.[362] Because the government surveillance in this case runs in direct contradiction of that original

353. *See* United States v. Jones, 132 S. Ct. 945, 954 (Sotomayor, J., concurring); Denniston, *supra* note 348.

354. *Jones*, 132 S. Ct. at 951 n.3.

355. *Id.* at 950 ("[J]ones's *Fourth Amendment* rights do not rise or fall with the *Katz* formulation.").

356. *See id.* at 950–51.

357. *Id.* at 952.

358. *See id.* at 950.

359. *See id.* at 951-52.

360. *Jones*, 132 S. Ct. at 952. "Karo accepted the container as it came to him, beeper and all, and was therefore not entitled to object to the beeper's presence, even though it was used to monitor the container's location." *Id.* (citing On Lee v. United States, 343 U. S. 747, 751–52 (1952)).

361. *Id.* at 951–52.

362. *Id.* at 950 ("As explained, for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ("persons, houses, papers, and effects") it enumerates.").

and, more fundamental, formulation of Fourth Amendment protection, a slim majority of the Court's members found the *Katz* inquiry unnecessary in resolving the present case.

Despite concurring in judgment, the opinion written by Justice Alito, with whom Justices Ginsburg, Breyer, and Kagan join,[363] functions almost as much as a dissent, offering unvarnished critique of the majority's trespass rationale. Justice Alito arranges his critical commentary into two parts. First, in sections I and II of the opinion, he questions strongly the Court's basic doctrinal premise—that the trespass rule is still controlling law in light of *Katz*.[364] Though the question of the trespass rule's renewed vitality merits exploration in its own right, the second line of Justice Alito's critique,[365] for the purpose of this article, raises the more relevant ideological schism among the Court's voting blocs. In this second line of critique, Justice Alito offers a distinctly contrasting vision of how the Fourth Amendment should operate in the context of technology-enhanced surveillance. Though Justice Alito never applies the "mosaic" label to his rationale, his formulation invokes identical policy concerns and conceptually tracks the rule design articulated by Judge Ginsburg in *Maynard*.[366] Justice Alito, applying a functionally equivalent approach to the "mosaic theory," ultimately reaches the same conclusion as the D.C. Circuit—that four weeks of warrantless GPS surveillance fails to accord with society's reasonable expectations of privacy, regardless of whether any physical intrusion or technical trespass occurred.[367]

Justice Alito opens this line of reasoning by first articulating what he sees as the basic problem of applying trespass logic to long-term surveillance. The trespass rule, in Justice Alito's words, "disregards what is really important (the *use* of a GPS for long-term tracking) and instead attaches great significance to something most would view as relatively minor . . . ."[368] Taken to its logical conclusion, the newly resurrected trespass rule would create normatively discordant results. In a trespass paradigm, any warrantless observation in public space, even if only for a moment, would

363. *Id.* at 957 (Alito, J., concurring).

364. *See id.* at 957–61 (Alito, J., concurring).

365. *See id.* at 961–64 (Alito, J., concurring).

366. *Compare Maynard*, 615 F.3d 555–67, *with Jones*, 132 S. Ct. at 961–64 (Alito, J., concurring);

367. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring); *see also What's the Status of the Mosaic Theory After Jones?*, *supra* note 26 (observing that Justice Alito's reasoning echoes that of the D.C. Circuit's in *Maynard*).

368. *Jones*, 132 S. Ct. at 961 (Alito, J., concurring).

be prohibited, so long as it was coupled with some, even slight, physical intrusion; however, surveillance executed through technology that successfully circumvented any technical trespass could go on indefinitely without any judicial oversight. To Justice Alito and the concurring members, such a result does not accord with the Fourth Amendment and the reasonable privacy expectations of the public.

Citing to *Knotts*, Justice Alito writes that "[r]elatively short-term monitoring of a person's movements on public streets [does] accord[] with expectations of privacy that our society has recognized as reasonable." Presumably, that is because the Court, in its long litany of settled cases, including *Katz*, *Karo*, and *Knotts*, has treated publicly exposed conduct as something presumably beyond the Fourth Amendment's reach.[369] However, Justice Alito distinguishes between "[r]elatively short-term monitoring" versus the multi-week surveillance presented in *Jones*.[370] The basis for this distinction is premised on the constitutionally determinative inquiry from *Katz*: what would society reasonably expect?[371] Echoing Judge Ginsburg's analysis from the circuit opinion, Justice Alito asserts that "[s]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not secretly monitor and catalogue every single movement of an individual's car for a very long period" of time.[372] Rather than laws of the legislatures or the courts, society's privacy expectations have historically been shaped and better-served by laws of physics and the limits of practical technology. [373] Consider that even if colonial-era agents of the British Crown had had an interest in attempting to acquire an equivalent volume and type of data as collected through GPS technology, they could only have done so through the most extraordinary and essentially unimaginable means.[374]

However, accounting for the practical limitations of surveillance abilities and resources is not solely the province of colonial history. Beeper monitors, like those used in *Knotts* and *Karo*, were not passive technologies that eliminated the need for human surveillance.[375] To the contrary, those

369. *See id.* at 964 (citing *Knotts*, 460 U. S., at 281-282).

370. *See id.* (Alito, J., concurring).

371. *See id.*

372. *Id.*

373. *See id.* at 963.

374. *Jones*, 132 S. Ct. at 959 n.3 ("The Court suggests that something like this might have occurred in 1791, but this would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience.").

375. *See id.* at 963.

technologies, though considered state-of-the-art at that time, still required an intense commitment of human and other resources that was far more consistent with traditional low or no-tech surveillance.[376] GPS and other emerging surveillance technologies provide the government with qualitatively different data collection capabilities that the public would not likely anticipate in a free society.[377] Working from that premise, Justice Alito concludes that four weeks of GPS-based surveillance "surely" crossed a constitutional threshold.[378] The law enforcement conduct in the present case, therefore, having intruded upon the public's reasonable privacy expectations, must be characterized as a search, presumably requiring prior judicial authorization.[379]

In the final opinion of the *Jones* case, Justice Sotomayor writes separately to set forth the most expansive view of privacy held by any member of the Court.[380] First, she expressly acknowledges her decision to join the Court's opinion and explains her concurrence with its trespass-based rationale.[381] She finds that "a search within the meaning of the Fourth Amendment occurs, at minimum, 'where, as here, the Government obtains information by physically intruding on a constitutionally protected area.'"[382] She finds the application of that base-line principle alone sufficient to decide the *Jones* case.[383] Despite finding the present case resolved through the application of a trespass approach, she parts from the Court's opinion by then engaging in a conversation with Justice Alito regarding the limits of the "trespass rule" and the application of *Katz*.[384] To this point, Justice Sotomayor not only endorses the view taken by Justice Alito that longer term GPS monitoring would in most cases impinge on expectations

376. *Id.* at 963 n.10.

377. *See id.* at 964.

378. *Id.*

379. *See id.*; United States v. Flores-Lopez, 2012 U.S. App. LEXIS 4078, at *10 (7th Cir. Ind. Feb. 29, 2012). Both Justice Scalia and Justice Alito found that the government had forfeited an alternative argument that the surveillance, even if characterized as a search, was "reasonable" and, therefore, not subject to the Fourth Amendment's warrant requirement. *See id.* at 964 n.11 (Alito, J., concurring). In fact, shortly after the *Jones* decision, Judge Posner wrote that a "minimally invasive search may be lawful in the absence of a warrant, even if the usual reasons for excusing the failure to obtain a warrant are absent, a holding that is implied by [*United States v. Robinson*, 414 U.S. 218 (1973)] and survives *Jones*, which declined to decide whether the search entailed in attaching a GPS device requires a warrant." *Flores-Lopez*, 2012 U.S. App. LEXIS 4078, at *10.

380. *See* Goldstein, *supra* note 349.

381. *See Jones*, 132 S. Ct. at 954 (Sotomayor, J., concurring).

382. *Id.* (quoting Justice Scalia at 953, n.3).

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

384. *Id.*

of privacy, but continues by questioning why short-term GPS surveillance should not also be subject to similar normative scrutiny.[385] Justice Sotomayor observes that GPS surveillance, regardless of the duration of its use, poses unique problems that she would find relevant "when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements."[386] First, GPS surveillance collects precise, comprehensive data that reveals the entirety of one's movements, including many activities that people expect to be able to engage in discreetly or with some sense of anonymity.[387] Second, this technology collects more information at a reduced cost when compared to conventional surveillance techniques.[388] Third, improvements in data storage technology provide the government with the capability to efficiently store, organize, and mine the voluminous amounts of collected data for years to come.[389]

As important as these recited factual assumptions are, Justice Sotomayor is not the first member of the judiciary to take notice of the improved capabilities of surveillance technology. In fact, judicial writers of all stripes, including those opposed to a doctrinal expansion of *Katz* through a "mosaic" or other analogous approach, seem to concede the proposition that enhanced surveillance technology consequently reduces individuals' practical ability to keep things secret.[390] The debate then is to determine whether this new reality has any constitutional significance and, if so, how to articulate a rule which responds to those concerns. As previously described, Justice Alito's opinion thoroughly discusses his view of the constitutional problem; however, his opinion only discusses rule design and application in abstract terms, never offering a theory on how to calculate when a surveillance operation has gone on too long.[391] Though Justice Sotomayor's opinion clearly endorses the factual observations and legal conclusions made by Justice Alito,[392] her opinion makes two distinctive moves that speak forcefully to rule design.

First, she views the misuse of such technologies as inimical to democ-

385. *See id.*

386. *Id.* at 956 (Sotomayor, J., concurring).

387. *See Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (citing for example People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

388. *Id.* at 956 (Sotomayor, J., concurring).

389. *Id.*

390. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 33–34 (2001).

391. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring). Instead, Justice Alito simply shifts the constitutional risk to the government, counseling law enforcement that it can simply seek a warrant in order to resolve any uncertainty. *Id.*

392. *See id.* at 955 (Sotomayor, J., concurring).

ratic society, because they would likely chill the exercise of constitutionally protected freedoms.[393] Surveillance technologies are not constitutionally problematic simply because they can collect more information more easily. Rather, the mode of observation, in and of itself, has a deleterious effect on human behavior.[394] Recall for a moment the problems illustrated by Bentham's and Foucault's "Panopticon" thought experiments—regardless of whether the warden watches or not, people's behavior changes when they believe they can be surreptitiously watched at any time without knowing it.[395] The challenge in the case of surveillance technology then is to determine how the government's apparently ubiquitous ability and willingness to observe and record individuals' conduct, especially lawful conduct, alters society and its relationship with its government.[396] In deciding cases of non-trespassory surveillance, Justice Sotomayor suggests that she would resolve the question by asking "[w]hether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[397] This formulation of how to assess the reasonable expectation of privacy, if ever adopted by the Court, would infuse the *Katz* test with a new constitutional referent—the jurisprudence of individual liberties and freedoms.[398] Consider that writers and members of the Court have long criticized *Katz* for its circularity and lack of substance.[399] For this reason, Justice Scalia and others have advocated the position that reasonable expectations of privacy cannot be adjudged without reference to a source of law outside the Fourth Amendment, usually citing to property law as the quintessential enabling source of law.[400]

---

393. *Id.* at 956.

394. *See id.* ("I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques.") (citing *Kyllo*, 533 U.S. at 35 n.2).

395. SLOBOGIN, *supra* note 2, at 92 ("[H]e who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power;...he becomes the principle of his own subjection.") (quoting MICHEL FOUCAULT, DISCIPLINE AND PUNISH 202–03 (Alan Sheridan trans., Vintage Books 2d ed., 1995)).

396. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (citing *Cuevas-Perez*, 640 F.3d at 285 (Flaum, J., concurring)).

397. *See id.* at 956 (Sotomayor, J., concurring).

398. *See generally* SLOBOGIN, *supra* note 2, at 98–106 (laying out several civil liberties based arguments for extending Fourth Amendment protection against public surveillance).

399. *See, e.g., Kyllo*, 533 U.S. at 34; *Jones*, 132 S. Ct. at 962 (Alito, J., concurring) (citing Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring)).

400. *See Kyllo*, 533 U.S. at 34; *Carter*, 525 U.S. at 97 (Scalia, J., concurring); *see also* Rakas v. Illinois, 439 U.S. 128, 143 (1978) ("Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal

What Justice Sotomayor articulates then is an analytical framework that fully responds to this concern by identifying a new referent. She strongly implies that related constitutional principles, such as expressive, religious, and associative freedoms, can provide the Fourth Amendment with objective reference points for judging society's reasonable privacy expectations.[401] Rather than relying solely on the tenets of property law, Justice Sotomayor identifies the preservation of constitutionally guaranteed liberties as the basis for regulating powerful new search technologies.[402] Though she never gives a particular label to her rationale, it bears a strong resemblance to *Maynard* "mosaic" approach.[403] And unlike either Justice Alito or Judge Ginsburg, Justice Sotomayor articulates the beginning of a rule that is not only doctrinally coherent, in that it references recognized constitutional principles in its analytical design, but can also account for the normative concerns raised by present-day and future surveillance technologies.

CRITICISMS OF "MOSAIC THEORY"

Knotts Controls

Commentary on the D.C. Circuit's unveiling of the "mosaic theory" formulation has approached from one of two attacks. The first critique questions the doctrinal soundness of the "mosaic theory" in the context of the Court's previous Fourth Amendment cases. This line of critique asserts that that the holding from *Knotts*—that "[a] person traveling in an automobile on public thoroughfares has no expectation of privacy in his movements . . . ."—is well-established and should control without exception, regardless of the technological or temporal circumstances of a surveillance operation.[404] While many of these same critics recognize that the *Knotts* Court reserved judgment as to what it described as "dragnet" surveillance, they discount the applicability of that reservation under the present facts. Instead, critics argue that *Knotts* reserved judgment only as to the specific hypothetical problem of suspicionless mass surveillance of the public.[405] In

---

property law or to understandings that are recognized and permitted by society. . . .").

401. *See id.* at 956 (Sotomayor, J., concurring).

402. *Id.*

403. *What's the Status of the Mosaic Theory After Jones?*,, *supra* note 26.

404. United States v. Maynard, 615 F.3d 544, 556 (D.C. Cir. 2010) (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)).

405. *Id.*; *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Moni-*

support of this view of the "dragnet" surveillance reservation, critics point the Court's decision in *United States v. Karo*, decided only a year after *Knotts*, in which the Court passed on a potential opportunity to scrutinize lengthy, warrantless surveillance of persons suspected of criminal conduct.[406] In the course of coming to its decision, the *Maynard* court had to make several novel and, therefore, controversial moves in dealing with this apparently controlling line of precedent.

Anticipating these critical observations, the *Maynard* court took a broad view of the *Knotts* "dragnet" surveillance question, concluding that the language encompassed concerns over the persistent surveillance of individual criminal suspects.[407] In support of this position, the court asserted that the *Knotts* "dragnet" question had to be viewed in light of the particular facts of that case.[408] Recall that in *Knotts*, the defendant was an individual suspected of criminal activity and tracked by law enforcement using a remote beeper device. Therefore, when the defendant made his objection concerning the potential for twenty-four hour surveillance of "any citizen of this country," it is hard to imagine how he could have made this objection to the exclusion of his own factual position.[409] Adding weight to this inference, Judge Ginsburg notes the Court implicitly accepted the objection in that context, as it directly quoted from Knotts's brief when it discussed this objection in its decision.[410] Whether this is a highly persuasive position is difficult to say. However, the ambiguity of the "dragnet" reservation certainly did not prohibit Judge Ginsburg's interpretation, which he ultimately employed in order to work around the holding from *Knott*.

Justice Alito, in his concurring opinion in *Jones*, also distinguishes *Knotts* from the present case and does so in two respects. First, he expressly contrasts the technologies presented in *Knotts* and *Karo* from the GPS technology in *Jones*.[411] Justice Alito observes that the beeper tech-

---

toring a Fourth Amendment Search, supra note 28; *D.C. Circuit Deems Warrantless Use of GPS Device and Unreasonable Search: United States v. Maynard, supra* note 28, at 833 (citing United Stated v. Karo, 468 U.S. 705, 719–21 (1984)).

406. *See D.C. Circuit Deems Warrantless Use of GPS Device and Unreasonable Search: United States v. Maynard, supra* note 28, at 833 (citing *Karo*, 468 U.S. at 719–21).

407. *Maynard*, 615 F.3d at 558.

408. *Id.* at 556–57 (citing *Knotts*, 460 U.S. at 283–84).

409. *See Maynard*, 615 F.3d at 556 ("[T]he Court was not only addressing but in part actually quoting the defendant's argument....The Court avoided the question whether prolonged 'twenty-four hour surveillance' was a search by limiting its holding to the facts of the case before it.") (quoting *Knotts*, 460 U.S. at 283).

410. *Maynard*, 615 F.3d at 556.

411. *See* United States v. Jones, 132 S. Ct. 945, 964 n.10 (2012) (Alito, J., concurring).

nologies employed in those older cases more closely resembled traditional surveillance, in that their use was sensitive to many of the same resource-dependent constraints that limited the overuse of standard human surveillance.[412] Second, Justice Alito finds that the holding from *Knotts* does not sweep as broadly as critics of a "mosaic" approach might assert. Rather, he distinguishes *Knotts* from the present case by asserting that *Knotts* only stood for the proposition that "relatively short-term monitoring of a person's movements on public streets" is consistent with society's reasonable privacy expectations.[413] Because *Jones* presents the problem of long-term surveillance conducted with highly advanced technology, *Knotts* is distinguishable and does not control.

Though neither the *Maynard* nor *Jones* decisions addressed the argument that *Karo* narrowed the "dragnet" reservation, the factual differences between both *Karo* and *Knotts* are consequential enough to undercut this position. In *Karo*, the surveillance operation was conducted pursuant to a judicial authorization. And even though the warrant was found to be insufficient to permit surveillance of the home, the Court never questioned the warrant's applicability to surveillance on public roads and spaces; therefore, the Court never truly had an opportunity in *Karo* to question warrantless surveillance of a suspect in publicly observable areas.[414] For that reason, *Karo* cannot so easily be read as an implicit resolution of the "dragnet" question reserved in *Knotts*.

The "Mosaic Theory" is Unworkable

Moving from the doctrinal to the practical, commentators have articulated several criticisms of the "mosaic theory" that can be grouped under the general heading of "unworkability."[415] In order to contextualize these criticisms, it is necessary to isolate exactly what rule *Maynard* asserts. First, the case reaffirms the general and well-accepted principle that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[416] Yet, measuring what is "exposed" is primarily where the "mosaic theory" achieves its innovation. The principle

412. *Id.*

413. *Id.* at 964.

414. *See* United States v. Karo, 468 U.S. 705, 708, 718 (1984).

415. *See D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search, supra* note 28; *D.C. Circuit Deems Warrantless Use of GPS Device and Unreasonable Search: United States v. Maynard,, supra* note 28, at 833–34.

416. United States v. Maynard, 615 F.3d 544, 559 (D.C. Cir. (2010) (citing Katz v. United States, 389 U.S. 347, 351 (1967)).

announced can be summarized as follows: the whole of a person's movements over time are neither actually nor constructively exposed to public view, because there is no reasonable likelihood that a member of the public would observe the totality of another person's movements;[417] therefore, a person has a reasonable expectation of privacy in the totality of his or her public movements over the course of a period of time (a month in the case of *Maynard*), when the collection and aggregation of those movements could only have been accomplished through technological means.[418] Because both the *Maynard* decision and the *Jones* concurring opinions are largely written in the form of broad, normative narrative, to include discussions on various privacy principles from a wide range of cases and related constitutional principles, the "mosaic theory" as a doctrinal rule can be difficult to discern. The above-synthesized rule nonetheless encompasses what conceptually sets this case apart from others, in that it attempts to define a way of discerning some narrow range of public conduct that attains a measure of constitutionally protected privacy.

The difficulty of capturing the "mosaic theory," however, is indicative of the generalized form of the "unworkability" claim. From this perspective, "mosaic theory" critics find the D.C. Circuit's approach misguided, because, as they describe it, the decision unnecessarily complicates the well-settled, easy-to-apply rules from *Knotts* and *Karo* with a highly normative standard that has an unclear foundation in Fourth Amendment doctrine.[419] This criticism has some purchase as the tortured modern history of the Court's Fourth Amendment jurisprudence can, from one perspective, be described as an evolving struggle to isolate and balance the normative values of the Fourth Amendment with need for translating these principles into operational rules. In *New York v. Belton*, the Court openly acknowledged that translating the Fourth Amendment into *ex ante* rules law enforcement can predictably apply is an important interest at work in the development of its jurisprudence.[420] As violations of the Fourth Amendment are regulated by the exclusionary rule,[421] a remedy that clearly exacts a high price for constitutional malfeasance, there is a heightened sense the Court then has a correlative obligation to announce rules that are not only doctrinally cor-

417. *Id.* at 560.

418. *Id.* at 563.

419. *See D.C. Circuit Deems Warrantless Use of GPS Device and Unreasonable Search: United States v. Maynard*,, *supra* note 28, at 833–34.

420. *See Four Models of Fourth Amendment Protection*, *supra* note 30, at 528 (citing New York v. Belton, 453 U.S. 454, 458 (1981)).

421. *See* U.S. CONST. amend. IV; LAFAVE ET AL. *supra* note 36, at 126.

rect, but also operationally clear and practical in a law enforcement setting.

While this criticism is not without some merit, it tends to flip the question of constitutionality on its head. Prior to *Katz*, Fourth Amendment doctrine was, even if imperfect, clear: if there was physical trespass, there was a Fourth Amendment violation. However, when given the opportunity in *Katz* to choose between operational clarity and substantive correctness, the Court consciously established the primacy of the latter.[422] And, when the Court announced the *Katz* test, the same criticisms were made and, in fact, are still being made today.[423] The Court neither needs nor wants a strictly "workable" test for its analysis of the Fourth Amendment, because it has the requisite institutional competence to employ the normative test from *Katz* and discern specific iterative rules law enforcement can then put into operation.[424] There is legitimate pressure for appellate courts to announce clear search and seizure rules because of the irrevocably high cost exacted for actions that are largely adjudicated *ex post*.[425] However, the Court has never asked law enforcement to enter into a philosophical debate as to what constitutes society's reasonable expectations of privacy. Rather, the Court reserves that level of conceptual analysis for itself in order to determine whether a particular investigatory practice amounts to a "search" or a "seizure." By translating its normative analysis into a final pronouncement on whether some conduct is either a "search" or not, the Court "provides considerable certainty" to legal advisers and law enforcement operating in the field.[426] In fact, the *Knotts/Karo* framework, approvingly cited by critics of the "mosaic theory," is the product of this deductive process of distilling specific rules from normative principles.[427]

To levy the undifferentiated criticism of "unworkability" is a bit cheap, as a court cannot issue a one-size-fits-all regulatory manual in every decision. Should *Brown v. Board of Education* be criticized as "unworkable" for not including a detailed plan for school integration?[428] If cases

422. LAFAVE ET AL., *supra* note 36, § 3.2(a).

423. *See id.*; Kyllo v. United States, 533 U.S. 27, 34 (2001).

424. *See Four Models of Fourth Amendment Protection*, *supra* note 30, at 528–29 (stating that, in implementing the Fourth Amendment, courts turn to clear rules that law enforcement can "readily follow").

425. *See id.* at 527–28 (noting there is great pressure on courts to implement the Fourth Amendment utilizing "clear *ex ante* rules" instead of unclear "*ex post* standards" because of the high social costs associated with suppression).

426. *Id.* at 528 (arguing the standard "provides considerable certainty" by delineating investigative procedures that do not lead to the suppression of evidence obtained).

427. *See supra* Part III.A.

428. *See* WILLIAM N. ESKRIDGE, JR. & JOHN FEREJOHN, A REPUBLIC OF STATUTES: THE

such as *Katz* or *Brown* can be described as "unworkable," it would seem the criticism is really just a euphemism for describing the difficulty of exerting executive and legislative effort to implement a new constitutional principle. The conceptual principles from the *Maynard* decision and the *Jones* concurrences, similar to the subsequent treatment of *Katz*, would likely result in the creation of specific rules as those principles are cycled through the branches of government and refined in subsequent court decisions. In fact, despite its lengthy conceptual rationale, the *Maynard* court, as well as the Alito concurrence in *Jones*, did announce a specific rule—the government cannot remotely track a suspect's movements for a four-week period unless conducted pursuant to a warrant.[429]

However, a stronger and more specific form of the "unworkability" critique comes in two forms. The first is that the "mosaic theory" would have the effect of making constitutional surveillance practices, when applied over time, unconstitutional. In other words, it would make constitutional practices "retroactively unconstitutional."[430] This criticism is not unfair, given that neither the *Maynard* decision nor the *Jones* concurrences offer much guidance on the presumed number of days—or weeks—that warrantless surveillance could persist before it turned into an offending "mosaic" and, therefore, a "search."[431] However, this situation is not as untenable as it would first seem. Albeit a slightly different context, this mirrors the problem faced by the Court as a result of its decision in *Gerstein v. Pugh*. In *Gerstein*, the Court held that persons arrested without a warrant had a right to a "prompt" hearing in front of a neutral and detached magistrate.[432] While there was substantial debate after *Gerstein* about what "prompt" meant in practical terms, the Court subsequently remedied this in *County of Riverside v. McLaughlin*, when it held that a hearing that takes

---

NEW AMERICAN CONSTITUTION 56 (2010) ("The most that judges can usually do—and this is the glory of *Brown*—is to jump-start the political process by forcing a fundamental normative discussion when the political system has not been responsive.").

429. *See* United States v. Maynard, 615 F.3d 544, 564–65 (D.C. Cir. 2010) (citing, with approval, various state laws and court decisions, which recognize the use of a GPS device for a prolonged period of time as a search subject to the Fourth Amendment's warrant requirements).

430. *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, *supra* note 28.

431. Justice Scalia observes of Justice Alito's concurrence: "[I]t remains unexplained why a 4-week investigation is 'surely' too long . . . ." United States v. Jones, 132 S. Ct. 945, 954 (2012). He continues, "What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist?" *Id.*

432. Gerstein v. Pugh, 420 U.S. 103, 114 (1975) ("[T]he detached judgment of a neutral magistrate is essential if the Fourth Amendment is to furnish meaningful protection from unfounded interference with liberty.").

place within forty-eight hours of arrest was presumably reasonable.[433] Turning again to the specific facts in *Maynard* and *Jones*, these cases offer little practical guidance, aside from the four-week bright-line standard, that would assist law enforcement in translating the rule into operation. However, just as in *County of Riverside*, the Court can announce more specifically tailored rules and guidelines in the course of future litigation. Alternatively, in the absence of judicial action, the legislative branch could set policy, regulating the number of days government agents could use GPS technology to collect location data without a warrant. As one example, Congress, via the Foreign Intelligence Surveillance Act ("FISA"), restricts the Attorney General's authority to conduct warrantless electronic surveillance for an unlimited duration following a declaration of war.[434]

A final criticism of the "mosaic theory" is that it does not provide any formulation for determining the size and scope of a mosaic that would trigger Fourth Amendment scrutiny.[435] Defense attorneys, attempting to bring entire investigations within the scope of a "mosaic," could argue that the totality of an investigatory file reveals intimate insights and facts about a person that would otherwise be unavailable to members of the general public.[436] Consistent with the "mosaic" formulation, this argument has doctrinal purchase now, as no person would reasonably expect to be investigated and tracked by a member of the general public; therefore, any information collected as a part of a law enforcement investigation could be viewed as a product of a Fourth Amendment "search" and subject to warrant requirements. This argument foresees that if *Maynard* were extended to its logical extreme entire investigations could be subjected to more intense Fourth Amendment scrutiny with few guiding principles to assist law enforcement in avoiding pitfalls.[437] This is a serious critique; nevertheless, the *Maynard* court appears to anticipate this concern in attempting to limit

433. Riverside v. McLaughlin, 500 U.S. 44, 56 (1991) (establishing concrete constitutional grounds under *Gerstein* by providing the limit of forty-eight hours with flexibility in ascertaining any unavoidable delays).

434. 50 U.S.C. § 1811 (2010) ("Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.").

435. *See D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, *supra* note 28 (positing *Maynard* will place great emphasis on defining the "exact scope of the mosaic").

436. *See id.* (explaining that defense attorneys will argue that clients were subject to larger "mosaic" investigations in order to have evidence excluded from admission at trials).

437. *See id.* (discussing how the new standard may require courts to define what acts of law enforcement fall within and outside the definition of a mosaic investigation).

its holding to the specific context of extended GPS surveillance, reserving questions of prolonged visual or other surveillance.[438] Turning to *Jones*, even though Justice Alito's concurrence similarly attempts to limit the application of its rationale to lengthy, technology-driven surveillance, Justice Sotomayor's opinion illustrates how the "mosaic theory" and its logic, if applied broadly, can begin to extend well-beyond the specific facts of the present case. Regardless of any attempt to limit the application of "mosaic theory" rationale, the opinions from *Maynard* and *Jones* offer future criminal litigants a credible doctrinal foothold to argue for far greater court regulation over entire criminal investigations.

The Problems of the "Mosaic Theory" are Better Handled by Statute

In *Olmstead*, Justice Brandeis warned that "[a]dvances in the psychic and related sciences" might eventually allow government agents to read citizens minds.[439] Four decades later, when Justice Harlan criticized *Olmstead* and *Goldman* as being approaches founded in "bad physics as well as bad law," one gets the sense that he foresaw an ominous future on the horizon—one where technology would eventually work a complete end-run around an antiquated "trespass" paradigm.[440] Even as recently as *Kyllo*, Justice Scalia asserted it would be "foolish" to believe that technology has left citizens' expectations of privacy unaffected.[441] These cases are illustrative of an oft-employed "privacy lost" narrative in matters of search and seizure law. But the narrative of dread rarely ends on a completely desolate note. In a "darkest-before-the-dawn" literary move typical of Fourth Amendment writing, redemptive possibility can be found by judges and courts possessing the courage to act decisively to protect privacy.[442] This perspective incorporates at least two assumptions. First, that courts, acting in the form of constitutional rule, are the branch of government best suited to avert technology's potential encroachment upon privacy.[443] Sec-

438. United States v. Maynard, 615 F.3d 544, 566 (D.C. Cir. 2010) ("We reserve the lawfulness of prolonged visual surveillance.").

439. *See* Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

440. *See* Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring).

441. Kyllo v. United States, 533 U.S. 27, 33–34 (2005).

442. *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Action*, *supra* note 19, at 804 (quoting *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting)) ("[Justice] Brandeis urged in 1928 that to protect our liberties as technology advances, 'every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.'").

443. *Id.* at 857 n.337 (citing Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Trades Image and Identity*, 82 TEX.

ond, that legislative and executive branch actors have no impetus to protect privacy norms unless they believe that the courts will find some investigatory practice inimical as a matter of constitutional doctrine.[444] The *Maynard* opinion aptly illustrates the operation of these narratives, for it pushes the bounds of the Fourth Amendment to its doctrinal and even logical limits. The justification for such an ambitious approach must, at least in part, stem from the assumption that matters of privacy require a constitutional response.

However, that has not necessarily proved true. The narrative of technological doom has not translated into judicial action to slow the advance of surveillance technology. Despite the Supreme Court's largely permissive attitude towards the constitutional regulation of surveillance technology, it cannot empirically be claimed that surveillance technologies have saturated public space to a degree where human behavior has been markedly modified. If, in the absence of constitutional protection from the courts, privacy was supposed to inevitably erode with the advance of technology, why do Americans not already have government-mandated GPS chips installed in all vehicles or have tiny hover drones peaking into their homes? It may be that, as the Court implied in *Katz*, the judiciary really does not have a monopoly on the protection of privacy.[445] Instead, legislative and executive action, situated in the context of a political landscape, provides the bulk of Americans' privacy protections.[446] If that were not the case and law enforcement simply could employ surveillance technology to the limits of constitutional doctrine, then the bleak dystopian future imagined by Justice Brandeis should already have come to pass. While the D.C. Circuit takes great doctrinal pains to protect the public from an unregulated technology it perceives as dangerous, the question, in light of the legislative landscape, is whether the *Maynard* court needed to make such an effort. Consider the context of cell phone-based location and GPS technologies and how Congress has largely staved off constitutional rule-making in this area, because it has legislatively regulated these technologies so tightly that the Fourth

---

L. REV. 1349, 1363 (2004)); Nola K. Breglio, Note, *Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance*, 113 YALE L.J. 179, 215 (2003); William J. Fenrich, Note, *Common Law Protection of Individuals' Rights in Personal Information*, 65 FORDHAM L. REV. 951, 986–90 (1996)).

444. *See* SLOBOGIN, *supra* note 2, at 89.

445. *See Katz*, 389 U.S. at 350–51.

446. *See The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Action*, *supra* note 19, at 807 ("Although scholars tend to focus on the Fourth Amendment, the real privacy protection has more often derived from statutory law.").

Amendment is rarely implicated.[447]

Cell site location information ("CSLI"), like GPS technology, provides location information for a cell phone user. Though less precise than GPS, it is far more ubiquitous, because every cell phone is capable of being located by CSLI technology. When a cell phone is turned on, it communicates and "registers" with the closest available cell phone tower at constant seven-second intervals.[448] This happens passively and, therefore, occurs regardless of whether the user makes a call or substantially changes location.[449] As the cell phone user moves location, the phone continues to send out signals and "register" with whatever tower provides the strongest signal, which is presumably the closest tower.[450] Having registered with a new tower, the cell phone's relative location to that single tower can now be determined. Additionally, the service provider, by identifying which 120-degree face of the registered tower is receiving the cell phone's signals, can determine the cell phone's orientation relative to the tower.[451] Merely by identifying the registered tower and its orientation in relation to a particular phone, that cell phone's location can be narrowed to within 200 feet or less of its precise location at any specified time.[452] In urban areas, these measurements become much more precise, because cell phones register and send signals to multiple towers at any given moment. If at least three towers are receiving signals and can be used in this comparative assessment—called triangulation—CSLI technology can provide a near-pinpoint location.[453]

But CSLI technology is old news now, as the vast majority of cell phones purchased in the United States now come equipped with GPS.[454]

---

447. *See e.g.*, Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2701–2711 (2006).

448. *See* Patrick T. Chamberlain, Note, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745, 1752 nn. 34–35 (2009) (citing Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 426 (2007)).

449. *See id.* at 1752.

450. *See id.* at 1753 (citing Stephanie Lockwood, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 309 (2004)).

451. *See* Chamberlain, *supra* note 448, at 1754 (citing *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 590 (W.D. Pa. 2008)) (quoting McLaughlin, *supra* note 448, at 427).

452. *See id.*.

453. *See id.* at 1753 (citing McLaughlin, *supra* note 448, at 427).

454. United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) (citing CTIA Consumer Info, *50 Wireless Quick Facts*, *available at* http://www. ctia.org/consumer-

The commercial market has driven this capability, since many of the computer applications ("apps") popular with consumers require the phone's precise location.[455] Yet, with the trove of potentially useful location data available, it is not only commercial interests that see its value, but also law enforcement. In 2009 alone, Sprint estimated that it provided various law enforcement agencies approximately eight million pieces of customer location data.[456]

Unlike GPS data from manually placed receivers, cell-phone-based tracking information, including GPS-based data, is tightly regulated by statute. The Stored Communications Act ("SCA"), subsequently amended by the Communications Assistance for Law Enforcement Act ("CALEA"), prohibits "providers" of "electronic communications" from disclosing to law enforcement "a record or other information pertaining to a subscriber to or customer of such service," including CSLI or other location data, unless such disclosure is done pursuant to a warrant or other court order.[457] Generally, a magistrate judge will issue the court order if law enforcement shows "'there are reasonable grounds to believe that . . . the records or other information sought[] are relevant and material to an ongoing criminal investigation.'"[458] However, most courts have found this procedure can only be applied to historical location data.[459] In other words, if the data is occurring in real-time, then it cannot be conceived of as a stored electronic

---

info/index.cfni/AID/10323); Edward C. Baig, *Bad Direction for GPS Devices; Portable Gadgets Lose Ground to Smart Phones*, USA TODAY, Dec. 21, 2010, at 1B. Also, Justice Alito, in his concurrence, points to a report claiming that as many as 322 million wireless devices are in operation in the United States. *Jones*, 132 S. Ct. at 963 (Alito, J., concurring).

455. *See* Michelle Higgins, *Let Your Fingers Do the Driving*, N.Y. TIMES, Nov. 14, 2010, (Travel), at 3 (reviewing traffic apps that rely on user's location); Victor Zapana, *Authorities Can Track Cell Phones Anywhere*, PITT. POST-GAZETTE, June 8, 2009, at B-5 (discussing apps that can track a phone's location even when out of GPS range).

456. *See* United States v. Pineda-Moreno, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, J., dissenting) (citing Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, SLIGHT PARANOIA BLOG (Dec. 1, 2009), http://paranoia.dubfire. net/2009/12/8-million-reasons-for-real-surveillance.html).

457. 18 U.S.C. §§ 2702(a)(3), § 2703(a), (c)(A)–(B) (2006).

458. 18 U.S.C. § 2703(d)(2006); *see In re* Application of United States for Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 313 (3d Cir. 2010).

459. *E.g.*, *In re* Application of United States for Order Authorizing Installation and Use of Pen Register Device (*McGiverin*), 497 F. Supp. 2d 301, 309 (D.P.R. 2007); *In re* Application of United States for Order Authorizing Installation and Use of Pen Register Device (*Orenstein*), 396 F. Supp. 2d 294, 308 (E.D.N.Y. 2005); *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth. (*Smith*), 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005); *see* Chamberlain, *supra* note 448, at 1771 n.173 (asserting courts have been reluctant to apply standard to real-time data). The aforementioned cases are cited by Chamberlain, *supra* note 448, at 1771 n.173, as examples of where the courts interpreted the SCA as applying only to historical location data.

communication and, instead, is treated as a "tracking device."[460] If the data is treated as coming from a "tracking device" rather than from an electronic communication, then the SCA prohibits providers from disclosing the information pursuant to the lesser showing required for the court order procedure and, instead, mandates that disclosure only occur pursuant to a warrant supported by probable cause.[461] Though the distinction as to whether law enforcement must apply for a SCA court order or a regular warrant supported by probable cause is important, the more critical observation for this conversation is that cell phone location data of any kind cannot be disclosed to the government without some form of judicial oversight. Given the ubiquity of cell phones in modern life, it is fair to assert that protecting this type of location information from government acquisition serves as a substantial privacy protection. Additionally, this statute goes well beyond the protection afforded by constitutional doctrine. As *Lee*, *Katz*, *Knotts*, and other Supreme Court cases dictate, activities exposed to the public cannot, by their nature, enjoy Fourth Amendment privacy. However, as a policy matter, Congress made a decision to carve out a zone of exclusion in location data generated as a part of cell phone use. Where cell phone technology provided an ability to monitor individuals' movements, Congress stepped in with statutory action to prevent abuse.

The description of how CSLI and phone-based GPS are regulated also illustrates how privacy policy in this country is often made *despite* the action of courts, rather than because of it. For instance, Congress passed the Electronic Communications Privacy Act ("ECPA"), which included the SCA, subsequent to the Court's decisions in *Knotts*.[462] This means that at the time Congress undertook a substantial legislative effort to mandate judicial oversight over government collection of communications data, it had no constitutional dictate directing that it do so.[463] This chronology tends to undercut the assumption that Congress can only legislate surveillance technology when doing so in the shadow of judicial edict.[464] Looking at other

460. *See* Chamberlain, *supra* note 448, at 1775–76.

461. *See* 18 U.S.C. § 2510(12)(C) (2006) (defining "electronic communication" to exclude "any communication from a tracking device"); 18 U.S.C. § 3117 (2006) (defining "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object").

462. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848; United States v. Knotts, 460 U.S. 276 (1983).

463. *See* WAYNE R. LAFAVE ET AL. PRINCIPLES OF CRIMINAL PROCEDURE: INVESTIGATION 242 (2d ed. 2009) ("The SCA was enacted in 1986 when it was unclear how the Fourth Amendment would apply to stored computer network communications").

464. *See* SLOBOGIN, *supra* note 2, at 89 (noting some cities have independently adopted pub-

privacy statutes, the SCA is not the only example of Congress acting to enhance privacy protections in the absence of constitutional mandate. For instance, Congress enacted the Right to Financial Privacy Act,[465] despite the Court's explicit holding that such records warranted no constitutionally recognized privacy protections.[466]

Of course, significant examples of Supreme Court decisions driving legislative action also exist. For instance, even though both the House and Senate had pending bills pertaining to the regulation of wiretaps and electronic surveillance prior to the Court's decision in *Katz*, the development of those legislative efforts and their final product, the Wiretap Act ("Title III"),[467] were in substantial part shaped by the progress and outcome of the *Katz* litigation.[468] Additionally, when the Supreme Court strongly signaled in *United States v. United States District Court for the Eastern District of Michigan*[469] that the government would have to conduct domestic national security surveillance in compliance with Fourth Amendment principles, Congress passed FISA.[470] As a measure aimed at preventing further opportunity for Supreme Court interpretation of the Fourth Amendment in national security cases, FISA succeeded by forcing the government to obtain warrants in a highly regulated process that closely mirrored the measures

---

lic surveillance rules that are voluntary and nonbinding).

465. Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697 (current version at 12 U.S.C. §§ 3401-3422).

466. *See The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Action*, *supra* note 19, at 856 (citing United States v. Miller, 425 U.S. 435, 443 (1976)) (finding the disclosure of bank records did not violate a depositor's Fourth Amendment rights because the depositor takes the risk that the information will be conveyed to the Government).

467. 18 U.S.C. §§ 2510–2522 (2006); *see The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Action*, *supra* note 19, at 850 ("[The Wiretap Act] is often referred to as 'Title III' because it passed as the third section of the mammoth Omnibus Crime Control Act of 1968.").

468. *See The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Action*, *supra* note 19, at 849-51; United States v. Jones, 132 S. Ct. 945, 962–63 (2012) (Alito, J., concurring) ("[C]oncern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping.")

469. United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div., 407 U.S. 297, 321 (1972).

470. Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1885(c) (2010); LAFAVE ET AL., *supra* note 463, at 246–47 (discussing the protective standards afforded by the Fourth Amendment regarding domestic security surveillance, the Supreme Court's interpretation of these standards, and Congress's subsequent enactment of FISA); *Electronic Surveillance—Congress Grants Telecommunications Companies Retroactive Immunity from Civil Suits for Complying Suits for Complying with NSA Terrorist Surveillance Program—FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436*, 122 HARV. L. REV. 1271, 1271–72 (2009).

required for Title III warrants in domestic criminal investigations.[471]

The lesson of these previous examples is that *Maynard* and *Jones*, rather than settling the issue of regulation of surveillance in public space, are really just the first effort. Analogous to the "reasonable expectation of privacy" from *Katz*, the "mosaic theory" or any similar formulation really tends to raise at least as many questions as it resolves. As Justice Alito suggests, the abstraction of these approaches tends to prove the wisdom of Chief Justice Taft's assertion from *Olmstead* that the regulation of surveillance technology is a matter that may be best left to Congress.[472] Therefore, good public policy may ultimately require legislative resolution in order to refine the "mosaic theory's" normative principles into functional rules. Potential legislative approaches available to policymakers in the wake of the *Maynard* and *Jones* opinions fall into one of at least a couple of models, which can be employed either individually or in combination with each other in order to provide the preferred policy response.

First, Congress could control surveillance of public space through legislation that regulates the use of specific technologies or surveillance modalities. For example, in the specific context of location data, several states have enacted statutes that expressly provide for judicial oversight of law enforcement's use of mobile tracking devices, including GPS technology.[473] Though the Court has expressed doubt as to whether state law can support a theory of privacy derived from the United States Constitution,[474] this limitation only applies to federal courts attempting to locate precedential value in state law. Outside the context of the courts, congressional policymakers should look to legislative approaches taken by the states as

471. *See* LAFAVE ET AL., *supra* note 463, at 247 (describing FISA regulations requiring the Executive Branch to apply for and obtain a court order from one of the eleven U.S. District Court judges appointed to the Foreign Intelligence Surveillance Court in order to conduct foreign intelligence surveillance); *In re* Sealed Case, 310 F. 3d 717, 736–37 (Foreign Int. Surv. Ct. Rev. 2002); Legal Auths. Supporting the Activities of the Nat'l Sec. Agency Described by the President, 1 Op. O.L.C. 3 (2006), *available at* 2006 WL 6179901.

472. *Jones*, 132 S. Ct. at 963 (Alito, J., concurring).

473. *See* United States v. Maynard, 615 F.3d 544, 564 (D.C. Cir. 2010) (citing UTAH CODE ANN. §§ 77-23a-4, 77-23a-7, 77-23a-15.5 (2011); MINN. STAT. §§ 626A.37, 626A.35 (2011); FLA. STAT. §§ 934.06, 934.42 (2011); OKLA. STAT. ANN. tit. 13, §§ 176.6, 177.6 (West 2011); S.C. CODE ANN. § 17-30-140 (2010); HAW. REV. STAT. §§ 803-42, 803-44.7 (2011); 18 PA. CONS. STAT. § 5761 (2008)).

474. *See D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, *supra* note 28 (noting the *Maynard* court's reliance on state laws for a reasonable expectation of privacy appears to be foreclosed by *Virginia v. Moore*, 553 U.S. 164 (2008) and *California v. Greenwood*, 486 U.S. 35 (1988)).

"laboratories of democracy"[475] in order to develop a sense for the normative and regulatory expectations of society in the context of surveillance technology. Building upon these individual state examples, Congress could also look to presently controlling federal law for both linguistic and normative guidance.

For example, the U.S. Code provides policy direction as to what constitutes a "mobile tracking device."[476] Even though this law, by itself, is only jurisdictional,[477] policymakers have successfully incorporated it by reference into other substantive statutory frameworks, such as the SCA and its regulation of government collection of historic and real-time location data.[478] These statutes together provide ready material for the expression of a more comprehensive statutory prohibition against warrantless tracking. Similar to the previously described state and federal examples, 18 U.S.C. § 3117 could be amended to include a substantive provision or could be incorporated into a separate congressional act in order to expand the regulation of electronic data collection. For example, the recently introduced Geolocation Privacy and Surveillance Act ("GPS Act") employs this drafting technique, incorporating the well-settled definition of a "mobile tracking device" into its substantive framework regulating the interception, disclosure, and use of "geolocation information."[479] Such an expansion of federal law makes normative sense, as there would seem to be little policy rationale for allowing the government's choice of surveillance modalities to frustrate Congress's objectives in the SCA of preventing unregulated government collection of location data.

In another example of how legislative action could focus on a specific surveillance modality for regulation, Congress could draft and enact an *Unmanned Aerial Surveillance Act.* Such an Act could also track the statutory approach taken by Title III and require that UAS surveillance only be conducted pursuant to a specific UAS warrant.[480] Substantively, the Act could define and then prohibit any "surveillance" from an "unmanned aerial system," unless conducted pursuant to a judicial order. The term "surveillance" would include collection of audio, visual, or other ambient data

475. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

476. 18 U.S.C. § 3117

477. 18 U.S.C. § 3117(a) (1986).

478. 18 U.S.C. § 2510(12)(C) (2002) (defining "electronic communication" to exclude "any communication from a tracking device" as defined in 18 U.S.C. § 3117).

479. S. 1212, 112th Cong. § 2 (2011) (currently referred to Senate Judiciary Committee and pending in House Subcommittee on Crime, Terrorism and Homeland Security as H.R 2168).

480. 18 U.S.C. §§ 2510–2520.

or digital information. The term "unmanned aerial system" would include any aviation platform controlled by any remote or artificial means. In order to receive a UAS warrant, the procedural requirements could then mirror the specialized warrant process mandated by Title III.[481] Finally, this act could tailor its regulatory scheme to explicitly permit warrantless UAS use when responding to exigencies or other special needs, such as search and rescue, natural disaster response, terrorist attack response, border surveillance, and immediate tactical support of high-risk law enforcement or national security operations.

While specific regulation of a particular technology offers the advantage of precision, it may also prove ineffective over time as technologies advance and change. Therefore, a second approach would be to attempt a more comprehensive legislative scheme aimed at regulating broader classifications of electronic surveillance activity. In fact, this is the regulatory design employed in the currently pending GPS Act, which prohibits the collection, disclosure, and use of an entire class of data—"geolocation information."[482] Another example of this broader regulatory design can be found in Title III, which prohibits the "aural" acquisition of any oral communication through electronic or other similar devices unless judicially authorized.[483] This means that government agents cannot augment their ability to hear or preserve oral communications without judicial oversight. As one commentator has suggested, an approach similar to Title III could also be enacted to prevent warrantless "visual surveillance."[484] While it is clear that Title III textually regulates interception of oral communications,[485] it is not at all clear, as a policy matter, why visual surveillance should not be regulated in a similar manner. As a general proposition, televising or videotaping someone's activities without his or her knowledge is at least as intrusive as eavesdropping on their private conversations.[486] The legislative record of Title III does not indicate any policy-based distinction between the regulation of visual and aural surveillance.[487] In reality, Title III's omission of visual surveillance from its regulatory scheme is simply a

481. *Id.*
482. S. 1212, 112th Cong. § 2 (2011).
483. 18 U.S.C. §§ 2510(2), 2510 (4), 2511 (2) (2011).
484. *See* SLOBOGIN, *supra* note 2, at 75–76.
485. *See* United States v. Torres, 751 F.2d 875, 880 (7th Cir. 1984) (citing 18 U.S.C. §§ 2561(1), 2518(1), 2511–13, 2515, 2517, 2519).
486. *See id.* at 878.
487. *See id.* at 880–81 (citing 18 U.S.C. § 2510(4)).

consequence of the technological landscape in 1968.[488] As *Katz* illustrates, wire intercept technology had at that time advanced to a point where it could be surreptitiously deployed. Because no similar visual surveillance capability existed at the time of Title III's enactment, there would have been no policy impetus to regulate such technology in advance of its development.[489] This regulatory omission should, therefore, be viewed as a mere circumstance of history rather than as a purposeful expression of society's values regarding sensory enhancing surveillance technology.

Additionally, to amend Title III so that it regulates visual as well as other forms of electronic surveillance would harmonize the substantive standards regulating domestic criminal investigations with FISA's broad regulatory treatment of electronic surveillance in national security cases. Enacted ten years after Title III, FISA substantially mirrors Title III's judicial oversight procedures.[490] However, one significant difference is in the breadth of the surveillance technology regulated by the respective statutes. While Title III only prohibits the unregulated interception of oral communications,[491] FISA contemplates judicial oversight over the use of any electronic, mechanical, or other surveillance device employed in order to monitor or acquire oral communications, as well as information "*other than* from a wire or radio communication . . . ."[492] This implies that FISA would regulate a wider variety of surveillance technologies under its framework, including technologies designed to collect visual or geolocation data.[493] While FISA does not regulate the conduct of domestic criminal investigations, it does provide a meaningful statement of national policy that calls into question whether Title III's narrow regulatory jurisdiction reflects current public policy.[494]

CONCLUSION

In the litigation over GPS surveillance, both the Supreme Court and the D.C. Circuit responded to a growing tension between surveillance technology, constitutional doctrine, and normative values. The D.C. Circuit,

488. *See id.*
489. *See id.*
490. *See e.g.*, LAFAVE ET AL., *supra* note 463, at 246–47.
491. 18 U.S.C. § 2511(1) (2010).
492. 50 U.S.C. § 1801(f)(4) (2010) (emphasis added).
493. *See Torres*, 751 F.2d at 881–82. Judge Posner, writing for the court, asserts the expansive language in FISA would place television surveillance under the statute's regulatory control. *Id.*
494. *See id.* at 881.

using the primary tool at its disposal—constitutional doctrine—articulated an expansion of *Katz* that would restrict the warrantless collection of informational "mosaics." Reviewing the D.C. Circuit's "mosaic theory," a majority of Supreme Court members strongly signaled their endorsement of this expansion of constitutional doctrine. Nonetheless, constitutional rule is only one modest tool for protecting privacy. In fact, even as Justice Alito and others on the Court voiced their open support for a *Maynard*-style expansion of Fourth Amendment doctrine, Justice Alito openly acknowledged that congressional regulation may ultimately prove more effective. While the Court creates constitutional doctrine in the course of resolving cases that come before it, it is not the sole branch of government responsible for setting policy that implicates constitutional values. As demonstrated by congressional regulation of other surveillance technologies and techniques, the legislative branch has proved capable of assuming a regulatory role in this field. Unlike the judiciary, it can integrate normative and other policy interests in generating tailored yet dynamic responses to a rapidly shifting technological landscape.[495] Legislative action, in combination with judicial expressions of constitutional doctrine, will result in credible, coherent, and durable policy that will "[g]ive society a chance of controlling the energies let loose by science and technology."[496]

495. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring). "A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." *Id.*

496. ARTHUR M. SCHLESINGER, JR., THE CYCLES OF AMERICAN HISTORY 422 (Houghton Mifflin Co. & First Mariner Books eds. 1999).