Mosaic Theory and the Fourth Amendment: How Jones Can Save Privacy in the Fact of Evolving Technology

Madelaine Virginia Ford
American University Washington College of Law

Follow this and additional works at: http://digitalcommons.wcl.american.edu/jgspl

Part of the Constitutional Law Commons

Recommended Citation
MOSAIC THEORY AND THE FOURTH AMENDMENT: HOW JONES CAN SAVE PRIVACY IN THE FACE OF EVOLVING TECHNOLOGY

MADELAINE VIRGINIA FORD*

I. Introduction ..........................................................................................1352
II. Background .........................................................................................1354
   A. The Supreme Court and the Evolution of Privacy
      Jurisprudence ..................................................................................1354
   B. Warrantless GPS Tracking and the Lower Courts .........................1356
      C. United States v. Maynard .............................................................1358
         1. Facts ......................................................................................1358
         2. Opinion ..................................................................................1358
   III. Analysis ............................................................................................1360
      A. The Supreme Court Should Use Jones to Examine the Issue It Reserved in Knotts and Affirm the D.C. Circuit Court’s Decision That Knotts Does Not Control In Cases Involving Comprehensive and Sustained Surveillance. ........1360
      B. The Supreme Court Should Affirm the D.C. Circuit Court’s Decision Because the Warrantless Use of a GPS Tracker Constituted an Unreasonable Search as Jones Had a Reasonable Expectation of Privacy in the Whole of His Movements over a Month, and Society is Willing to Accept This Expectation as Reasonable .............................................1362
         1. The D.C. Circuit Court Correctly Held That Jones Had a Reasonable Expectation of Privacy in the Whole of His Movements over a Month Because His Movements Were Not Exposed to the Public in Light of the Mosaic Theory. ..................................................................................1363
         2. The D.C. Circuit Court Correctly Held That Jones’ Reasonable Expectation of Privacy in the Whole of His

* J.D. candidate at American University Washington College of Law. Thank you to the Journal of Gender, Social Policy & the Law for its support and the faculty of Washington College of Law for its guidance.
I. INTRODUCTION

Every day millions of individuals worldwide depend on the Global Positioning System (GPS) to provide location, timing, and navigational services. While GPS provides many significant benefits to society, the scope and detail of the information that law enforcement can collect using GPS creates individual privacy risks because its use may impinge on individuals’ Fourth Amendment rights to be free from search and seizures.

Law enforcement officials describe GPS devices as an efficient, safe, and accurate way to track vehicle movement and laud the quality of information the devices gather. The information law enforcement officials collect using GPS tracking devices creates a highly credible and permanent record of evidence for criminal prosecutions. Furthermore, as the cost of GPS use becomes more affordable, law enforcement agencies will use GPS more frequently.

Despite the growing use of GPS in law enforcement investigations, few laws restrict the government’s use of GPS tracking. The Supreme Court has yet to examine the constitutionality of governmental use of GPS.
devices under the Fourth Amendment. The United States Congress has also refrained from limiting law enforcement’s investigatory uses of GPS devices.8

In United States v. Maynard, the United States Court of Appeals for the District of Columbia held that police use of GPS tracking devices without a warrant is an unconstitutional search.9 The Maynard decision differed from other circuit court decisions in which courts held that warrantless police use of GPS devices did not constitute a search.10 Maynard’s holding is significant because it established the rule that the police use of GPS devices is a search and, therefore, implicates Fourth Amendment protections.11 As GPS technology raises important Fourth Amendment concerns, the Supreme Court will likely clarify the constitutionality of law enforcement’s GPS use.12

GPS devices involve evolving technology within our modern society.13 The unresolved question is whether privacy law can keep up with this technological advancement.14

7. See United States v. Knotts, 460 U.S. 276, 283-84 (1983) (noting that the Court left open the question of comprehensive sustained monitoring in deciding the case); see also United States v. Maynard, 615 F.3d 544, 556 (D.C. Cir. 2010) (highlighting the Supreme Court’s distinction between a discrete and limited search such as a beeper and sustained monitoring or “mass surveillance”), cert. granted sub nom. United States v. Jones, 131 S. Ct. 3064 (June 27, 2011) (No. 10-1259).


9. See Maynard, 615 F.3d at 563 (declaring the police search unreasonable and in violation of the Fourth Amendment).

10. See, e.g., id. at 558 (holding that the warrantless use of GPS by the police constituted a search); United States v. Pineda-Moreno, 591 F.3d 1212, 1217 (9th Cir. 2010) (ruling that the police did not conduct an impermissible search of the defendant’s car by monitoring his location with mobile tracking devices); United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010) (finding the GPS installation reasonable because it was not random, arbitrary, invasive, and did not track private places); United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007) (ruling that using GPS is the equivalent to following a car and is not a search).


12. See H.W. Perry Jr., Deciding to Decide: Agenda Setting in the United States Supreme Court 251 (1991) (“A circuit split is not simply a formal criterion for cert.; it is probably the single most important criterion . . . .”); see also Spencer S. Hsu, Appeals Court Limits Use of GPS to Track Suspects, WASH. POST, Aug. 7, 2010, at A4, available at http://www.washingtonpost.com/wp-dyn/content/article/2010/08/06/AR2010080604946.html (proclaiming that the D.C. Circuit opinion has cleared the way for Supreme Court review of the issue of warrantless GPS tracking for an extended period of time).


Part II of this comment examines the Supreme Court’s privacy framework that controlled the decisions of the circuit courts and illuminates the divided nature of both state and federal courts on the issue of warrantless GPS tracking. Part III argues that *United States v. Knotts* should not be controlling in cases of continuous and prolonged GPS monitoring. Part III further contends that the D.C. Circuit Court’s use of the “mosaic theory” presents a new workable theory for Fourth Amendment analysis. This Comment finally considers the policy implications of evolving technology and the Fourth Amendment with a focus on the disparate impact of the issue on Muslim Americans.

II. BACKGROUND

A. The Supreme Court and the Evolution of Privacy Jurisprudence

Several significant Supreme Court decisions specifically address the issue of technology and its implications for an individual’s Fourth Amendment right to privacy. *Katz v. United States* articulated the two-part standard for a reasonable expectation of privacy under the Fourth Amendment stating that an individual must have a subjective expectation of privacy that society finds reasonable. The decision also establishes that what an individual seeks to preserve as private, even in a public area, may have constitutional protections. Courts have used this standard to

Knotts?] (explaining the status of the Fourth Amendment interpretations and evolving technology).

15. See infra Part II (framing the Supreme Court’s privacy jurisprudence and noting the lower courts review of GPS tracking).

16. See infra Part III.A (arguing that the Supreme Court specifically excluded prolonged monitoring from the issues decided in *Knotts*, making the case an unsuitable precedent).

17. See infra Part III.B (arguing that the mosaic theory, which postulates that discrete pieces of information when combined together, adopt a new significance based on the collective picture the information presents, is a workable test in examining evolving technology and privacy).

18. See infra Part IV (noting the current issues related to government GPS use and Muslim Americans).

19. See *Kyllo v. United States*, 533 U.S. 27, 35 (2001) (holding that information obtained by thermal imaging of a suspect’s home constituted a search); *United States v. Knotts*, 460 U.S. 276, 281 (1983) (deciding that police use of a beeper on a drum in a suspect’s vehicle was not a search as there was no reasonable expectation of privacy); *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (delineating the required elements to establish a reasonable expectation of privacy).

20. See *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (comparing how people have a subjective expectation of privacy for a conversation in their home but not outside the home where others can overhear).

21. See id. at 351 (reiterating that the Fourth Amendment protects people, not places, and that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to
analyze subsequent privacy jurisprudence.\textsuperscript{22}

Another seminal Supreme Court decision on the nature of privacy came in \textit{United States v. Knotts}.\textsuperscript{23} In \textit{Knotts}, police planted a beeper in a container of chemicals before the suspect purchased the container and placed it in his vehicle.\textsuperscript{24} The police used the beeper to trace the vehicle to a cabin owned by one of the suspects and obtained a warrant to search the premises.\textsuperscript{25} The Court focused on the diminished expectation of privacy in a vehicle that travels on public roadways and found that the beeper surveillance was not a search.\textsuperscript{26} In \textit{Knotts}, the suspect’s argument centered on the police monitoring, and not on the installation of the beeper as a search.\textsuperscript{27}

The Supreme Court addressed the issue of evolving technology and privacy again, in \textit{Kyllo v. United States}.\textsuperscript{28} In \textit{Kyllo}, the government suspected Kyllo of growing marijuana in his home and used a thermal imaging device from outside Kyllo’s home to detect radiation from the marijuana cultivation lamps.\textsuperscript{29} The Court held that because the device was not in general public use and because the search explored details of the home that were previously unknowable without intrusion, the act constituted a search that required a warrant.\textsuperscript{30}

\footnotesize{\textsuperscript{22} See, e.g., \textit{Knotts}, 460 U.S. at 280 (accepting the Court’s holding in \textit{Katz} as controlling).}

\footnotesize{\textsuperscript{23} Id. at 281 (finding that a person has a diminished expectation of privacy in his vehicle and the use of a beeper to follow the person does not change that expectation).}

\footnotesize{\textsuperscript{24} See id. at 277-78 (explaining that police used a radio transmitter beeper without a warrant and without the consent of the suspect to collect locational information).}

\footnotesize{\textsuperscript{25} See id. at 278-79 (highlighting how the police warrant allowed the police to search the cabin, where they found a methamphetamine laboratory that they used to convict the suspect).}

\footnotesize{\textsuperscript{26} See id. at 281, 285 (“A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”).}

\footnotesize{\textsuperscript{27} See id. at 286 (Brennan, J., concurring) (predicting that the case would have been more difficult to decide had the suspect challenged the beeper’s original installation and detailing the holding in \textit{Silverman v. United States}, 365 U.S. 505, 509-12 (1961), which finds that if “the government does engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment even if the same information could have been obtained by other means”).}

\footnotesize{\textsuperscript{28} See \textit{Kyllo v. United States}, 533 U.S. 27, 40 (2001) (clarifying that the use of a thermal heat detector presumptively violated a person’s right to privacy in his home).}

\footnotesize{\textsuperscript{29} See id. at 29-30 (explaining that evidence from the thermal scan of the home provided evidence to procure a warrant which led to Kylo’s indictment).}

\footnotesize{\textsuperscript{30} See id. at 40 (instructing that the search was presumptively unreasonable without a warrant).}
B. Warrantless GPS Tracking and the Lower Courts

Multiple circuit courts have addressed the issue of warrantless GPS tracking. Various courts have specifically examined the issue of law enforcement’s installation and use of GPS tracking devices on an automobile without a warrant in the course of a police investigation. The court in United States v. Garcia coined the term “wholesale surveillance” to refer to the new technologies that might allow law enforcement officials an unprecedented ease and scope of surveillance. The decision warned that advancements in surveillance technology presented considerable threats to privacy but stated that the court did not need to resolve that momentous issue. Recent decisions in United States v. Marquez and United States v. Pineda-Moreno represent a similar desire to avoid the constitutional scrutiny involved in ruling that a search occurred. The Marquez decision echoed the concerns over wholesale surveillance, yet the court refused to find the warrantless use of the GPS tracker a search. The decision focused on the non-invasive nature of GPS trackers on an automobile, and the fact that police installed the GPS tracker after the suspect had parked the vehicle on a public road. The court in Pineda-Moreno also referred to Garcia in finding that the warrantless use of a GPS tracking device did not constitute a search.

31. See United States v. Maynard, 615 F.3d 544, 568 (D.C. Cir. 2010) (holding that the warrantless use of a GPS tracking device on a suspect’s automobile constituted a search and violated the Fourth Amendment), cert. granted sub nom. United States v. Jones, 131 S. Ct. 3064 (June 27, 2011) (No. 10-1259); United States v. Pineda-Moreno, 591 F.3d 1212, 1217 (9th Cir. 2010) (ruling that the warrantless use of a GPS tracking device on a suspect’s automobile was not a search); United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010) (deciding that the warrantless use of a GPS tracking device on a suspect’s automobile did not constitute a search); United States v. Garcia, 474 F.3d 994, 997-96 (7th Cir. 2007) (resolving that the use of a GPS tracking device on an automobile by law enforcement did not constitute a search).

32. Maynard, 615 F.3d at 549; Pineda-Moreno, 591 F.3d at 1213; Marquez, 605 F.3d at 607; Garcia, 474 F.3d at 995.

33. See Garcia, 474 F.3d at 998 (using the term “wholesale surveillance” to explain the capabilities of surveillance that new technology offers law enforcement officials).

34. See id. (emphasizing the importance of judicial review of wholesale surveillance).

35. See Pineda-Moreno, 591 F.3d at 1217 (concluding that monitoring the suspect’s automobile with the GPS device was not a law enforcement search); Marquez, 605 F.3d at 610 (finding that the GPS device “merely allowed the police to reduce the cost of lawful surveillance” and did not constitute a search).

36. See Marquez, 605 F.3d at 610 (quoting Garcia, 474 F.3d at 998, and adding that as technology advances, law enforcement’s ability to undertake massive and possibly arbitrary GPS data collection is a concern).

37. See id. (focusing on the public nature of the road to imply that people have lower expectations of privacy on the road).

38. See Pineda-Moreno, 591 F.3d at 1216 (quoting Garcia, 474 F.3d at 997) (“[F]ollowing a car on a public street . . . is unequivocally not a search within the meaning of the amendment.”).
officers attached a tracking device while the car was parked in the suspect’s driveway. The court reasoned that because the suspect did not take steps to exclude individuals from his driveway, he did not have a reasonable expectation of privacy in the driveway, and the use of the tracking device fell short of a search.

The D.C. Circuit Court’s decision in Maynard represents a significant jurisprudential shift regarding the consideration of GPS tracking as a search. The court in Maynard rejected the holdings of the other circuit courts and held that the police use of GPS tracking constituted a search under the Fourth Amendment.

In addition to the federal courts, state courts remain divided on the issue of governmental use of warrantless GPS tracking. State legislatures have attempted to create a clear guideline by enacting statutes that impose criminal penalties for GPS tracking and mandate the exclusion of GPS data evidence obtained without a warrant. The disparity in the law at both the state and federal levels further increases the likelihood that the Supreme Court will review the issue in order to provide greater consistency and prevent geographical injustice.

39. See id. at 1214 (repeating the suspect’s argument that the police violated his privacy when they entered his driveway to access his car).

40. See id. at 1215 (proclaiming that the suspect’s lack of active exclusion, such as barriers or enclosures, of others from his driveway negated his reasonable expectation of privacy in the space).

41. See United States v. Maynard, 615 F.3d 544, 555-56 (D.C. Cir. 2010) (holding that Knotts is not controlling and the warrantless use of a GPS tracking device on a suspect’s automobile was a search that violated the Fourth Amendment), cert. granted sub nom. United States v. Jones, 131 S. Ct. 3064 (June 27, 2011) (No. 10-1259).

42. See id. at 557-58 (rejecting the holdings in Pineda-Moreno, Marquez, and Garcia and noting that each court reserved the issue of whether “wholesale” surveillance requires a warrant).


44. See, e.g., FLA. STAT. ANN. §§ 934.31, 934.42 (West 2010) (mandating that police acquire a warrant before installing a mobile tracking device); MINN. STAT. ANN. §§ 626A.35, 626A.37 (West 2010) (requiring a court order for the use of any mobile tracking device); UTAH CODE ANN. §§ 77-23a-13, 77-23a-15.5 (LexisNexis 2010) (commanding that police acquire a warrant before using a mobile tracking device).

45. PERRY, supra note 12, at 250 (stating that Supreme Court review is likely as it will be equitable to have a clear Supreme Court ruling instead of conflicting circuit court opinions).
**C. United States v. Maynard**

1. **Facts**

   During the course of a drug investigation, law enforcement officials placed a GPS tracking device on Antoine Jones’ Jeep, which tracked Jones’ movements twenty-four hours a day for twenty-eight days. In the District Court, Jones argued that while police had an order for the installation of the device, there was a lack of probable cause, the order had expired before police installed the device, and the police attached the device outside of the issuing court’s jurisdiction. The District Court held that the government was not required to obtain a court order or a search warrant to install a GPS device on a vehicle. The District Court suppressed the GPS data that police collected while Jones’ car remained in his garage. The District Court convicted Antoine Jones and Lawrence Maynard of conspiracy to distribute and to possess with intent to distribute five kilograms or more of cocaine and fifty grams or more of cocaine base.

2. **Opinion**

   The Circuit Court consolidated the appeals of Maynard and Jones, and after finding that none of the joint issues warranted reversal, focused on Jones’ individual argument. The court rejected the government’s contention that *Knotts* was controlling, specifically pointing to the Supreme Court’s distinction between the limited information collected by a beeper during a single discrete journey, and more comprehensive sustained monitoring. The Circuit Court applied a *Katz* analysis and determined that unlike movement in a single journey, the totality of an individual’s movements over the period of a month is not actually exposed to the

---


47. See *Jones*, 451 F. Supp. 2d 71 (noting that the Government contended that even if it did not issue a warrant, Jones had no reasonable expectation of privacy in his vehicle that would prevent the installation of the GPS device).

48. See *id.* (referring to the holding in *United States v. Koro*, 468 U.S. 705, 715 (1984), where the Supreme Court excluded evidence that police collected while the beeper was in a private residence because of the reasonable expectation of privacy in the home).

49. See *id.*

50. See *Maynard*, 615 F.3d at 548.

51. See *id.* at 549.

52. See *id.* at 555-56 (emphasizing the Supreme Court’s reservation of whether a warrant would be required in the case of twenty four hour surveillance or “drag-net” surveillance and noting the single 100-mile trip involved in *Knotts*).
public, because the chance of anyone observing all of the movements is extremely unlikely.\(^{53}\)

The court also applied the mosaic theory, which posits that discrete pieces of information when combined together, adopt a new significance based on the collective picture the information presents.\(^{54}\) In applying this theory of information, the court held that an individual does not constructively expose the whole of his or her movements.\(^{55}\)

The government typically advances the mosaic theory in Freedom of Information Act cases.\(^{56}\) This theory has increased in prominence since the September 11, 2001 attacks.\(^{57}\) The D.C. Circuit Court used the mosaic theory to justify an individual’s expectation of privacy in his or her continuous and prolonged movements.\(^{58}\) This theory provides an interesting option in addressing the current dilemma that courts face in attempting to reconcile Fourth Amendment interests with evolving technology.\(^{59}\)

The D.C. Circuit Court determined that society recognized Jones’ expectation of privacy in all of his movements over the course of a month, and that utilizing a GPS device without a warrant in order to monitor his movements defeated his reasonable expectation of privacy.\(^{60}\) The court reversed Jones’ conviction because the court found that the police procured

---

53. Id. at 560.

54. See United States v. Marchetti, 466 F.2d 1309, 1318 (4th Cir. 1972) (defining the mosaic theory by stating that “[t]he significance of one item of information may frequently depend upon knowledge of many other items of information. What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context.”).

55. See Maynard, 615 F.3d at 562 (“The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life . . . .”).


57. See id. at 631 (explaining that while not all courts have sanctioned the mosaic theory, several high profile rulings have used the mosaic theory to sustain government secrecy).

58. See also Maynard, 615 F.3d at 562-63 (using the mosaic theory to find that prolonged surveillance implicates privacy in a way that discrete surveillance does not).


60. See Maynard, 615 F.3d at 563 (“A person does not leave his privacy behind when he walks out his front door” and that the application of Katz leads to the conclusion that society recognizes the privacy in an individual’s total movements in a month).
evidence in violation of the Fourth Amendment.61

Following the release of the decision, the prosecution petitioned for a rehearing en banc in the D.C. Circuit Court, which the court denied.62 The case was further appealed to the United States Supreme Court, which granted certiorari.63

III. ANALYSIS

A. The Supreme Court Should Use Jones to Examine the Issue It Reserved in Knotts and Affirm the D.C. Circuit Court’s Decision That Knotts Does Not Control In Cases Involving Comprehensive and Sustained Surveillance.

The Court in Knotts specifically reserved the issue of twenty-four hour or “dragnet” surveillance when it examined the Fourth Amendment implications of warrantless police use of a beeper.64 Subsequent lower court decisions relied on Knotts to uphold warrantless prolonged GPS surveillance even though the Court had limited its holding to exclude this type of surveillance.65 These decisions distinguished wholesale surveillance, which the Seventh Circuit described as police using GPS to track thousands of cars at random, from prolonged surveillance of an individual.66 In Maynard, the court noted that the Supreme Court decision in Knotts clearly referred to prolonged surveillance of an individual as the Court was responding to the defendant’s argument regarding surveillance of an individual.67 The Court’s language in Knotts indicates that the Court

61. Id. at 568.

62. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), reh’g en banc denied, 625 F.3d 766 (D.C. Cir. 2010) (denying the petition for a rehearing en banc in a 5 to 4 vote).


64. See United States v. Knotts, 460 U.S. 276, 284 (1983) (“[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.”).

65. See, e.g., United States v. Marquez, 605 F.3d 604, 609 (8th Cir. 2010) (using Knotts to reason that an automobile traveling from one place to another has no reasonable expectation of privacy); United States v. Pineda-Moreno, 591 F.3d 1212, 1216-17 (9th Cir. 2010) (relying on Knotts to hold that the use of a GPS device did not constitute an impermissible search); United States v. Garcia, 474 F.3d 994, 996 (7th Cir. 2007) (noting that the Court in Knotts held that use of a beeper was not a search).

66. See Garcia, 474 F.3d at 998; see also Maynard, 615 F.3d at 557 (outlining that the circuit courts had misinterpreted the question reserved in Knotts as only applying to mass surveillance).

67. See Maynard, 615 F.3d at 556 (describing the defendant’s argument that “twenty-four hour surveillance of any citizen of this country will be possible, without
reserved the issue of prolonged individual surveillance for the future. This makes *Knotts* unacceptable precedent for questions involving the warrantless and continuous GPS tracking of individuals.\(^{68}\)

*Knotts* also signifies that persons traveling on public roads in their vehicles lack a reasonable expectation of privacy in their movements from one location to another.\(^{69}\) This case indicates that a person lacks a reasonable expectation of privacy in discrete trips, such as a single trip; however this case does not indicate that individuals lack a reasonable expectation of privacy in the totality of their movements.\(^{70}\) The police in *Maynard* used GPS technology to track Jones’ movements continuously for a month, not simply from one location to another.\(^{71}\) Consequently, the rule derived in *Knotts* did not apply and should not control cases of prolonged GPS monitoring because the rule implicates a discrete trip rather than prolonged monitoring.\(^{72}\)

GPS devices are considerably more intrusive than the beeper used in *Knotts* and warrant independent judicial privacy analysis.\(^{73}\) When law enforcement investigators use beepers, they must use visual surveillance, beepers, or sense-augmenting equipment in order to track the suspect.\(^{74}\) Beepers malfunction in inclement weather and require immense financial and manpower investment.\(^{75}\) GPS devices, on the other hand, provide a minute-by-minute record of surveillance, can be used in any weather condition, are not labor-intensive or expensive for police to use, and do not require constant visual surveillance to track a signal.\(^{76}\) *Knotts* involved the use of significantly less invasive technology, and therefore should not control cases involving GPS devices as the use of GPS devices allows for prolonged and highly intimate intrusions into individuals’ privacy.\(^{77}\)

\(^{68}\) See *Knotts*, 460 U.S. at 283-84 (reserving the issue of twenty-four hour surveillance of an individual and not mass or wholesale surveillance); *Maynard*, 615 F.3d at 557-58 (urging that *Knotts* is not controlling in cases of prolonged warrantless surveillance of an individual).

\(^{69}\) *Knotts*, 460 U.S. at 281.

\(^{70}\) See *Maynard*, 615 F.3d at 557 (rejecting the government’s argument that *Knotts* refers to any and all movement of a vehicle in public).

\(^{71}\) See id. at 558.

\(^{72}\) See id. at 556-57 (explaining that the roughly hundred-mile journey in *Knotts* is critically different from highly invasive prolonged monitoring).

\(^{73}\) See Brief for Appellants at 53-68, United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) (No. 08-3030), 2009 WL 3155141, at *39-47.

\(^{74}\) Id. at *41 (classifying the capabilities of the beeper discussed in *Knotts* and the GPS device at issue in *Maynard*).

\(^{75}\) Id.

\(^{76}\) See id. at *56-58 (explaining the superiority of surveillance capability of the GPS device compared to a beeper).

\(^{77}\) See *Tied up in Knotts?*, supra note 14, at 453-54 ("To suggest that the
Maynard presents the opportunity for the Supreme Court to examine the issue specifically reserved in Knotts.78 The discrete nature of the monitoring and the use of a less advanced surveillance device make Knotts an incompatible precedent for cases involving prolonged warrantless GPS tracking.79 A Supreme Court affirmation of the holding in Maynard will signal to both state and federal courts that Knotts is not precedent in cases involving warrantless prolonged monitoring by law enforcement.80

B. The Supreme Court Should Affirm the D.C. Circuit Court’s Decision Because the Warrantless Use of a GPS Tracker Constituted an Unreasonable Search as Jones Had a Reasonable Expectation of Privacy in the Whole of His Movements over a Month, and Society is Willing to Accept This Expectation as Reasonable.

Supreme Court privacy jurisprudence dictates that courts undertake a Katz analysis to determine whether a search was reasonable under the Fourth Amendment.81 The two-prong test dictates that Fourth Amendment protections apply when an individual has both an objectively and subjectively reasonable expectation of privacy in his or her actions.82 The D.C. Circuit Court used the mosaic theory to establish that Jones had a reasonable expectation of privacy in his aggregated whereabouts for the month that he was under surveillance.83 The court then turned to the second prong of the Katz test and relied on state law trends and specific state cases to find an objectively reasonable expectation of privacy.84


79. See id. at 556-58 (holding that Knotts applies to cases involving discrete monitoring and not to cases involving wholesale surveillance); Brief for Appellants at 56-58, United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) (No. 08-3030), 2009 WL 3155141 at *56-58 (comparing the superior technological capabilities of a GPS device to a beeper).

80. Cf. Savage, supra note 11 (hypothesizing a Supreme Court review of Maynard due to the contradicting decisions of lower courts).


82. Id.

83. See Maynard, 615 F.3d at 562-63 (using the mosaic theory to conclude that collective movements reveal more than discrete trips and that an individual has a reasonable expectation of privacy in their collective movements).

84. See id. at 563-64 (holding that the action of the state legislatures, specific state cases, and the highly invasive nature of a GPS search indicate that society would be willing to recognize Jones’ expectation of privacy in his collective movements as reasonable).
Ford: Mosaic Theory and the Fourth Amendment: How Jones Can Save Privac
2011] MOSAIC THEORY AND THE FOURTH AMENDMENT 1363

presence of an objectively and subjectively reasonable expectation of privacy implicated Fourth Amendment protections and required the court to reverse Jones’ conviction as the GPS tracking constituted an unreasonable search.85

1. The D.C. Circuit Court Correctly Held That Jones Had a Reasonable Expectation of Privacy in the Whole of His Movements over a Month Because His Movements Were Not Exposed to the Public in Light of the Mosaic Theory.

The D.C. Circuit Court correctly held that Jones had a reasonable expectation of privacy in the totality of his movements twenty-four hours a day for twenty-eight days.86 Maynard expressly presents the issue of whether wholesale surveillance of an individual requires a warrant.87 The court successfully used the mosaic theory to establish that Jones had a reasonable expectation of privacy from such surveillance.88

The first prong of the Katz test addresses whether an individual has exposed information to the public and what that individual can reasonably expect others to do with that information.89 Jones’ movements in his vehicle may have been on public roads, but the likelihood that another individual would observe all of his movements is effectively nil.90 Maynard is consistent with Supreme Court precedent because, while an individual may be able to gather the information, the fact that a reasonable person would not expect another to record his collective and prolonged movements preserves the expectation of privacy.91

The Supreme Court has previously reviewed and upheld government use of the mosaic theory to protect collective information.92 While the

85. See id. at 568 (recognizing that without the evidence obtained through warrantless police use of GPS data, the evidence was insufficient).
86. See id. at 558 (differentiating the recording of the totality of one’s movements from piecemeal tracking).
87. See id. at 557-58 (distinguishing other circuit courts that have preserved the constitutional limits to GPS tracking).
88. See id. at 562 (justifying a reasonable expectation of privacy in collective movements under the mosaic theory).
89. See United States v. Katz, 389 U.S. 347, 351 (1967) (explaining that a reasonable expectation of privacy depends on the degree to which an individual exposes information to the public).
90. See Maynard, 615 F.3d at 559-60 (describing that Jones did not actually expose his movements to the public).
91. Compare Bond v. United States, 529 U.S. 344, 338-39 (2000) (holding that a bus passenger has a reasonable expectation that his bag will not be felt in an exploratory manner, even though the bag is in a public space), with Maynard, 615 F.3d at 560 (contending that an individual has a reasonable expectation that his prolonged and continuous movements, while they may be in a public area, will not be observed).
government originally used the mosaic theory to defeat the rationale for the Freedom of Information Act, it has expanded the use of the theory to justify closing deportation hearings, indefinitely detaining non-citizens, and searching certain records.93 Judges have extended extreme deference to the government in many instances when the government has asserted the mosaic theory as a justification for intelligence secrecy.94 Scholars note that even though the government often provides little evidence in support of the mosaic theory aside from vague national security claims, judges frequently side with the government for fear of “unknown vulnerabilities.”95 Mosaic theory cases emphasize the critical value of collective information and evidence a judicial fear of discrete pieces of information compromising the collective.96

The fear of the unknown value of collective information should also protect an individual’s fundamental right to privacy from highly intrusive government searches.97 Just as judges refused to allow the diffusion of discrete pieces of information in the name of unknown national security interests, they should also protect the value of an individual’s collective information.98 Individual privacy, like national security, is a critical aspect of free society and warrants heightened protection for collective information.99

The mosaic theory of information aligns real world expectations about privacy with the rule of law.100 GPS technology enables law enforcement to conduct surveillance that would be too expensive to collect using other

93. See id. at 869-70 (describing the broad scope of activities in which the government invokes the mosaic theory to keep activities private).
94. See id. at 852-55 (arguing that judges, fearing national security implications, showed extreme deference to the government in allowing it to protect non-classified information).
95. See Pozen, supra note 56, at 653-54 (suggesting that judges protect the government).
96. See, e.g., Halperin v. CIA, 629 F.2d 144, 150 (D.C. Cir. 1980) (“We must take into account, however, that each individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself.”).
98. See, e.g., Halperin, 629 F.2d at 150 (justifying the protection of CIA legal bills under the theory that someone could combine them with other discrete information to uncover covert CIA transactions).
99. Id.
100. See Sanchez, supra note 59 (positing that the mosaic theory of information and privacy is preferable to an analysis which assumes that the sum of “public” facts must always be itself a public fact).
methods. The massive amounts of data accumulated by GPS devices, when viewed collectively, provides a highly detailed profile of an individual, including not only where he or she goes, but also his or her political, religious, professional, and romantic associations. An individual reasonably expects his or her movements to be disconnected and anonymous, and the intimate portrait of his or her life that police are able to compile through continuous monitoring, undermines that reasonable expectation of privacy.

The mosaic theory is a novel theory in the Fourth Amendment context and it could dramatically change privacy jurisprudence. Legal scholars have been promoting the mosaic theory, which some refer to as the “aggregation effect,” as a new way to think about personal information in the digital age. The flexibility of the mosaic theory provides advantages to courts because the test can adapt to evolving technology in a way that other tests would be unable to do.

The significant strength of the theory is also its biggest weakness: judges measure a search not by whether a particular individual act is a search but by whether the collective conduct amounts to a search. This presents concern because no bright line rule exists that would distinguish a non-search from a search when examining data collected by a GPS tracking device.

Maynard differs from Knotts in that Knotts involved a single,
discrete trip where *Maynard* involved prolonged monitoring. The court neglected to articulate the bright line between a single discrete trip and a month of continuous monitoring.

The mosaic theory supports Jones’ reasonable expectation of privacy in the totality of his movements for the month during which he was under warrantless surveillance. While the mosaic theory is not without flaws, further judicial development of the theory’s Fourth Amendment implications will likely resolve these issues. The flexibility of the mosaic theory provides a standard that is capable of addressing individual privacy concerns in the face of rapidly advancing surveillance technology.

2. The D.C. Circuit Court Correctly Held That Jones’ Reasonable Expectation of Privacy in the Whole of His Movements over the Period of a Month is One Which Society is Prepared to Accept as Reasonable, as Evidenced by State Legislation and Specific State Cases.

The D.C. Circuit Court, in examining *Maynard* under the second prong of the *Katz* test, correctly held that society would recognize Jones’ expectation of privacy as reasonable. To determine what society is willing to accept as reasonable, courts must look to societal norms, the law of previous judges, and legislative intent. The movement of state legislatures towards providing protection from warrantless police use of GPS tracking devices is a strong indication of the fact that society agrees that this type of intrusion violates an expectation of privacy. State court would not).


110. See Kerr, *supra* note 104 (“One-month of surveillance is too long, the court says. But how about 2 weeks? 1 week? 1 day? 1 hour?”).

111. See *Maynard*, 615 F.3d at 562-63 (using the mosaic theory to satisfy the first prong of the *Katz* test and to establish a subjective reasonable expectation of privacy).

112. See Sanchez, *supra* note 59 (addressing the flaws of the mosaic theory but positing that the theory remains workable regardless).

113. See id. (lauding the flexibility of the mosaic theory in terms of addressing privacy concerns of evolving technology).

114. See *Maynard*, 615 F.3d at 563-64; see also *Katz*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (noting the requirement that society views the privacy expectation as reasonable).


116. See, e.g., *Utah Code Ann.* § 77-23a-15.5 (LexisNexis 2010) (providing that an investigative or law enforcement officer needs a court order to install any mobile tracking device and stating that the there must be specifically granted authority to attach a tracking device to any area in which there exists a reasonable expectation of
cases also indicate a trend toward judicial acceptance of an objectively reasonable expectation of privacy in the totality of individuals’ prolonged movements in their automobile. Therefore, warrantless GPS monitoring defeats an expectation of privacy.

Additionally, requiring a warrant for law enforcement use of GPS devices is consistent with existing societal norms. A recent survey of societal privacy concerns relating to location-indicating programs on cellular telephones revealed that individuals believed that risks associated with the use of such technology outweighed the benefits. These results indicate society’s unease with the intrusiveness of GPS tracking in public and private areas, as well as the fear of government abuse of the technology.

Applying the mosaic theory to Maynard strengthens the argument that society would be willing to accept Jones’ expectation of privacy as reasonable. Maynard and similar state cases differ from the decisions in Garcia, Marquez, and Pineda-Moreno because those decisions did not recognize the distinction between discrete and collective information in Knotts. Societal expectations of privacy will inevitably change based on the nature of a prolonged search and the mosaic of an individual that the


118. See Maynard, 615 F.3d at 563 (concluding that an objective expectation of privacy exists).

119. See Tied up in Knotts?, supra note 14, at 459 (arguing that requiring a warrant is consistent with existing norms and the free society envisioned by the Framers).

120. See Janice Y. Tsai et al., Location-Sharing Technologies: Privacy Risks and Controls, 6 I/S: J.L. & POL’Y FOR INFO. SOC’Y 119, 138-40, 145 (2010) (revealing that perceived risks of location sharing technology outweighed the benefits, such as finding individuals in an emergency or tracking missing children).

121. See id. at 145 (reporting that individuals in the survey expressed that both a fear of being tracked by the government and the overall lack of privacy as harms associated with GPS programs in cellular telephones).

122. See Maynard, 615 F.3d at 563 (warning that “prolonged GPS monitoring reveals an intimate picture of the subject’s life that he expects no one to have . . .”).

123. See United States v. Knotts, 460 U.S. 276, 284 (1983) (explicitly reserving the issue of prolonged surveillance stating that if such collective surveillance eventually occurs, the court may then determine whether alternate constitutional principles apply). Compare Maynard, 615 F.3d at 666-56 (recognizing that Knotts was inappplicable because it involved limited surveillance), with United States v. Pineda-Moreno, 491 F.3d 1212, 1216-17 (9th Cir. 2010) (holding that under Knotts, surveillance for a reasonable period of time was not a search), and People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009) (“Constant, relentless tracking of anything is now not merely possible but entirely practicable, indeed much more practicable than the surveillance conducted in Knotts.”).
collective information creates for law enforcement.\textsuperscript{124} Citizens do not reasonably expect that the government will track their continuous whereabouts without a warrant in order to create a highly detailed mosaic of their lives.\textsuperscript{125}

The sociological data, combined with the activity in state court and state legislatures, signals society’s fear of warrantless GPS tracking.\textsuperscript{126} These factors indicate that Jones had an objectively reasonable expectation of privacy in the totality of his movements for the month he was under warrantless surveillance.\textsuperscript{127} Therefore, warrantless GPS tracking in \textit{Maynard} constituted a search in violation of the Fourth Amendment as Jones had a subjectively and objectively reasonable expectation of privacy in the totality of his movements for a month.\textsuperscript{128}

IV. POLICY RECOMMENDATIONS

A Supreme Court affirmation of warrantless police use of GPS tracking to create detailed mosaics of individuals will change residents’ relationship with the government.\textsuperscript{129} Recent reports of warrantless government GPS tracking confirm the suspicions of the \textit{Maynard} court.\textsuperscript{130} Several recent stories illuminate how the government’s use of GPS tracking specifically targets Muslim-Americans in the wake in 9/11.\textsuperscript{131}

Yasir Afifi, a U.S. citizen and California resident, with an Egyptian-born father, was having his oil changed when his mechanic found a rectangular
device attached to the undercarriage of the automobile. Afifi posted pictures of the device on an online forum, where posters indicated that it was a GPS tracking device. Soon after, four armed FBI agents approached Afifi, demanding that he return the device as it was federal property. The FBI confirmed that it had placed the GPS device on Afifi’s vehicle, but did not indicate why the government was investigating Afifi. Comments made by the FBI agents indicated that Afifi was under surveillance for three to six months.

Abdo Alwareeth, another California resident, claims that a similar situation occurred two years ago when he found a GPS device on his vehicle while taking an auto-mechanics class. Alwareeth, a U.S. citizen originally from Yemen, cannot understand why, after forty years living in the United States, the government targeted him. Alwareeth and his wife now live in constant fear of FBI surveillance and check their vehicles daily for additional tracking devices.

Zahra Billoo, the head of the local chapter of the Council on American-Islamic Relations, explains that this type of FBI activity creates a rift between the government and American-Islamic communities by frightening these communities. Billoo also reported that two Ohio residents recently found similar tracking devices on their vehicles.

The most frightening aspect of these incidents is not the actual devices found, but the likelihood that the FBI and other law enforcement agencies are conducting warrantless GPS surveillance on unsuspecting residents. The opinions of the Seventh, Eighth and Ninth Circuit Courts deny any protection to individuals from the government’s warrantless use of GPS tracking even in situations such as these where the individuals were religiously or ethnically targeted. Muslims in the United States face

132. Id.
133. Id.
135. Kim, supra note 131.
137. Kim, supra note 131.
138. Id.
139. Id.
140. See id. (referring to the Islamic American and Arab American communities).
141. Zetter, supra note 136.
142. Cf. Barker, supra note 134 (asserting that it is highly unusual that Afifi’s device was found at all and implying that most GPS devices of this nature will not be found).
143. Cf. United States v. Pineda-Moreno, 591 F.3d 1212, 1217 (9th Cir. 2010)
growing discrimination in post-9/11 America. As the attitude in the United States continues to become increasingly negative towards Muslims, it is critical that warrants be required in order to prevent “Islamophobia” from infiltrating law enforcement practices. A Supreme Court affirmation of Maynard would provide a basic level of protection for Muslim-Americans, as it would require a minimum of probable cause for the government to use a GPS tracking device.

V. CONCLUSION

Individual privacy is a fundamental right and directly involves the ability to prevent the collection and circulation of personal information. The current Supreme Court privacy framework fails to account for the level of intrusion occasioned by advanced technology and how its use undermines privacy protections. Knotts should not control cases involving the continuous monitoring with GPS devices, as the case dealt with a discrete journey and specifically did not address the issue of prolonged surveillance. A warrantless police beeper used for a one hundred-mile trip and warrantless GPS tracking for a month or more are not equivalent

144. See, e.g., Steven Greenhouse, Muslims Report Rising Discrimination at Work, N.Y. TIMES, Sept. 24, 2010 at B1 (illustrating the rise in reported incidents of discrimination against Muslims in the workplace and noting the sixty percent increase from 2005 to 2009 in claims).


147. See SOLOVE, supra note 105, at 51 (equating the collection of personal information without an individual’s knowledge to powerlessness).


surveillance techniques and implicate separate privacy issues. As surveillance technology continues to evolve, the Supreme Court must reevaluate its reliance on *Knotts*, and *United States v. Jones* presents the ideal opportunity for the Court to do so.

The mosaic theory, while novel as a justification for Fourth Amendment protection, provides a practical alternative for privacy analysis that is flexible enough to adapt to developing technologies. Just as the government has successfully used the theory to protect the unknown value of collective information, citizens too, should be able to use this rationale to protect the unknown value of personal collective information. The adoption of the mosaic theory and the rejection of warrantless GPS searches by police have significant implications for the future of individual privacy and technology.

For example, built in vehicular GPS systems, which used to be present exclusively in luxury car models, are now prevalent in a large variety of standard vehicles. These built in “concierge systems,” such as OnStar, allow police officers to monitor the past and present location of these vehicles without installing a tracking device. For police, this eliminates issues of whether the installation of the tracking device constituted a search. A Supreme Court decision, allowing warrantless GPS tracking, could imply that law enforcement agencies do not need a warrant to collect information from built in GPS systems, which some state courts have

150. See *Maynard*, 615 F.3d at 556-57 (rejacketing *Knotts* as a controlling case because of the differences in technology and the nature of the privacy interest at stake).

151. Cf. *Tied up in Knotts?*, supra note 14, at 453-54 (“Where the sophistication of GPS technology permits the pinpoint tracking of persons (not just vehicles), the overly broad application of *Knotts* allows a substantial encroachment upon personal privacy that was clearly not envisioned by the *Knotts* Court.”).

152. See *Sanchez*, supra note 59 (lauding the mosaic theory’s flexibility as opposed to the current privacy analysis regime).

153. See *Maynard*, 615 F.3d at 562 (utilizing the mosaic theory to find that an individual has a reasonable expectation of privacy in the totality of their movements over a prolonged period); *Pozen*, supra note 56, at 653-54 (noting the government’s use of the mosaic theory to protect the uncertain value of collective information in secrecy cases).

154. See *Sanchez*, supra note 59 (arguing that the mosaic theory of privacy will be necessary in order to prevent Fourth Amendment protections from becoming obsolete in the face of advancing technology).

155. See Donald W. Garland & Carol M. Bast, *Is the Government Riding Shotgun? Recent Changes in Automobile Technology and the Right to Privacy*, 46 CRIM. L. BULL. 295 (2010) (opining that technological advances in recent years have lead to more cars being built with GPS and concierge systems).

156. See id. (arguing that concierge systems in automobiles potentially allow law enforcement tracking and eavesdropping capabilities).

157. See id. (proposing that because car manufacturers include GPS systems in vehicles, individuals would only have the opportunity to contest law enforcement’s use of the previously installed GPS devices).
already found to be a less invasive procedure.\textsuperscript{158}

It is likely that the Court’s decision will also impact future court cases involving a multitude of location sharing devices such as cellular phones, laptops, and other mobile devices.\textsuperscript{159} The Electronic Communications Act governs cell phone tracking and requires law enforcement to obtain a court order in order to obtain information about a person’s location.\textsuperscript{160} Lower courts lack a consensus on the issue of whether these orders require probable cause or simply an articulable facts standard.\textsuperscript{161} Supreme Court affirmation of the \textit{Maynard} decision would send a clear signal to law enforcement that a warrant is required to use an individual’s technological devices to determine his or her location.\textsuperscript{162}

The Fourth Amendment protects privacy in the relationship between the government and citizens.\textsuperscript{163} While the Court has shifted from a property and trespass regime of privacy evaluation, the current conceptualization of the Fourth Amendment fails to adapt to technological advances and changing society.\textsuperscript{164} Privacy jurisprudence must evolve to shield individuals’ lives and social practices as well as information that relates to humans’ basic needs and desires from inappropriate police uses of advanced technology.\textsuperscript{165} The mosaic theory provides a workable option that accommodates modern technology and allows adjustments to privacy jurisprudence.

\begin{itemize}
\item \textsuperscript{158} \textit{See id.} (explaining that the court, in United States v. Coleman, No. 07-20357, 2008 WL 495323 (E.D. Mich. 2008), found that the police were not required to install an additional tracking device because using the existing built in device was less invasive).
\item \textsuperscript{159} \textit{See Adam Koppel, Warranting a Warrant: Fourth Amendment Concerns Raised By Law Enforcement’s Warrantless Use of GPS and Cellular Phone Tracking, 64 U. MIAMI L. REV. 1061, 1069 (2010) (noting the need for Fourth Amendment guidance in light of the advances in mobile technology, such as cell phones).}
\item \textsuperscript{160} \textit{See 18 U.S.C. § 2518 (2006) (detailing the lawful procedure for intercepting electronic communications).}
\item \textsuperscript{161} \textit{See Koppel, supra note 159, at 1080-83 (exposing the courts’ inconsistent requirements for court orders).}
\item \textsuperscript{162} \textit{Cf. id. at 1089 (advocating that the Supreme Court address the issue of the warrant requirement in cases of GPS and cellular telephone tracking).}
\item \textsuperscript{163} \textit{See SOLOVE, supra note 105, at 191 (referencing Orwell’s and Kafka’s propositions that government intrusions into the privacy of an individual prevent freedom and well-being).}
\item \textsuperscript{164} \textit{See id. at 190 (arguing that while the Court has adjusted the privacy framework from a property based philosophy, the current jurisprudence is too narrow to afford the larger Fourth Amendment protections).}
\item \textsuperscript{165} \textit{See id. at 191 (proposing that privacy must protect individuals’ lives where judgment is particularly abrasive and in areas of our basic needs including sexuality, entertainment, political activity, and family).}
\end{itemize}