UIC John Marshall Journal of Information Technology & Privacy Law

Volume 32 | Issue 4 Article 1

Spring 2016

Rise of the Mosaic Theory: Implications for Cell Site Location Tracking By Law Enforcement, 32 J. Marshall J. Info. Tech. & Privacy L. 236 (2016)

Lance Selva

William Shulman

Robert Rumsey

ARTICLES

RISE OF THE MOSAIC THEORY: IMPLICATIONS FOR CELL SITE LOCATION TRACKING BY LAW ENFORCEMENT

LANCE H. SELVA*, WILLIAM L. SHULMAN**, & ROBERT B. RUMSEY***

ABSTRACT

The authors examine the unique legal and privacy implications that cell site location information tracking by law enforcement poses for current Fourth Amendment jurisprudence. Following a brief explanation of how cell phone tracking works, their discussion is directed to the concept of privacy under the Fourth Amendment both prior to and following the seminal Supreme Court decision of *Katz v. United States* (1967), including a review of the Supreme Court's historical treatment of tracking devices post-*Katz*. Consideration is then directed to the *United States. v. Maynard* (2010) decision, where the court employed the "mosaic" theory in a Fourth Amendment search framework and how its adoption of the mosaic has created a novel approach for broadening privacy protections. The authors maintain that the two concurring opinions endorsing a mosaic approach in the *United States v. Jones* (2012) GPS tracking decision suggest that the theory will have continuing vitality in shaping the debate between personal privacy and effective law enforcement as technology evolves.

* Lance Selva is a Professor and Interim Chair of Criminal Justice Administration at Middle Tennessee State University. He is also a criminal defense practitioner. He received his J.D. degree from the University of Alabama School of Law in 1975 and earned his Ph.D. from The Florida State University School of Criminology in 1984.

Correspondence regarding this article should be addressed to Lance Selva, Department of Criminal Justice Administration, Middle Tennessee State University, Box 238, Murfreesboro, TN 37132. E-mail: lance.selva@mtsu.edu.

** William Shulman is an Associate Professor of criminal justice administration at Middle Tennessee State University. Mr. Shulman worked as Public Defender in Nashville, Tennessee from 1986-1990. He received his J.D. degree from the University of Tennessee College of Law in 1975.

*** Robert Rumsey is engaged in the private corporate sector. He received his MCJ degree from Middle Tennessee State University 2013.

I. INTRODUCTION

There is perhaps no more omnipresent symbol of our modern, interactive society than the cell phone. It is estimated that some 320,000 million individuals in the United States actively subscribe with cell phone service providers.[1] That number represents triple the number of subscribers just a decade ago.[2] Perhaps the most distinguishing aspect of cell phones is that they allow us to be accessible to others at any given moment, whether at our office, in our car, at a restaurant or bar, or even in our bed. As one study found, forty-four percent of cell phone users slept with their phone next to the bed.[3] The ubiquitous nature of cell phones has not only altered the balance between work and life, where each of us is "available" for calls, texts, and emails, wherever we might be: they also have altered the balance between a citizen's "right to be left alone," as Justice Brandeis once entreated,[4] and the government's legitimate law enforcement goal of crime detection and prevention.

As cell phone location tracking by the government demonstrates, emerging technologies have the capability of constricting the notion of what constitutes a "reasonable expectation of privacy" for citizens,[5] particularly if they happen to venture into a public space. Cell site location tracking by law enforcement holds the potential, absent strict and transparent judicial oversight, to effectuate an on-going erosion of the boundaries of places and locations where individuals can enjoy personal solitude, escaping the shadow of governmental scrutiny.[6]

Cell phones and Global Positioning System (GPS) technology have provided the government and law enforcement agencies with mechanisms for almost unlimited and widespread covert surveillance activities through cell site location information tracking, both in historical and real-time terms.[7] There has been an increase in police requests and court orders to cell phone service providers for cell site location information [CSLI] without securing

---

1. CTIA-The Wireless Association's Annual Wireless Industry Survey (Dec. 2013), *available at* http://www.cita.org/your-wireless-life/how-wireless-works/annual; Matt Blaze, Testimony before House Subcommittee. Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services (June 24, 2010), *available at* http://w.w.w.crypto.com/papers/blaze-judiciary-20100624.pdf.

2. CITA, *supra* note 1.

3. Tanya Mohn, *Silencing the Smartphone*, N.Y. TIMES, B3 (January 1, 2013).

4. S.D. Warren & L.D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

5. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

6. Courtney E. Walsh, *Surveillance Technology and the Loss of Something A Lot Like Privacy: An Examination of the "Mosaic Theory" and the Limits of the Fourth Amendment,* 24 ST. THOMAS L. REV.169, 172 (2012); ALAN F. WESTIN, PRIVACY AND FREEDOM 31 (1967).

7. Brian Davis, *Prying Eyes: How Government Access to Third-Party Tracking Data may be Impacted by* United States v. Jones, 46 NEW ENG. L. REV. 843 (2012); Kevin McLaughlin, *The Fourth amendment and Cell Phone Tracking,* 29 HASTINGS COMM. & ENT. L.J. 421 (2007); Derek P. Richmond, *Can You Find Me Now?—Tracking the Limits on Government Access to Cellular GPS Location Data,* 16 COMMONLAW CONSPECTUS 283 (2007).

search warrants based on probable cause.[8] Some of the providers have resisted such requests, while more have handed over such information. Records indicate that service providers responded to a reported 1.3 million requests in 2011 alone.[9] The courts are placed in the position of having to determine the balance between the nature and quality of the intrusion on a person's Fourth Amendment interests and the legitimate needs and goals of law enforcement.[10]

Journalists, academics, and privacy advocacy groups have paid attention to GPS tracking for the last decade, during which time a number of state and federal courts issued decisions on the question of whether attachment and/or monitoring of a GPS tracking device to a vehicle violated Fourth Amendment privacy protections.[11] Some courts have viewed GPS tracking as not constituting a search, making a warrant unnecessary.[12] Other courts have held that a warrant based on probable cause was required in order to track a suspect.[13] It was not until the case of *United States v. Maynard* that a federal court took a wholly different approach to assessing the privacy interests at stake, the "mosaic theory."[14] This new approach adopted by the D.C. Circuit Court of Appeals considered the amount and type of information gathered by GPS tracking of a vehicle continuously over a 28 day time period, and held that such monitoring was a search in violation of the defendant's reasonable expectation of privacy.[15] The decision ran counter to every other federal court of appeals that had previously taken up the issue.

The Supreme Court subsequently granted certiorari in the case of *United States v. Jones* and thus set the stage for what would become a significant decision regarding privacy expectations in an advanced technological surveillance age.[16] Although the majority felt it unnecessary to employ the mosaic approach, basing its holding on narrower trespass grounds in concluding that an unreasonable search had taken place,[17] it was the two concurring opinions endorsing a mosaic approach that seem to have suggested that the theory has

---

8. William Curtiss, *Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency Across Statutory Regimes,* 45 COLUM. J.L. & SOC. PROBS. 139 (2011); Davis, *supra* note 7; Steven M. Harkins, CSLA Disclosure: Why Probable Cause Is Necessary to Protect What's Left of the fourth Amendment, 68 WASH. & LEE L. REV. 1875 (2011).

9. Eric Lichblau, *Cell Carriers Called on More in Surveillance,* N.Y. TIMES, A1 (July 9, 2012).

10. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment,* 111 MICH. L. REV. 311 (2012); *United States v. Place*, 462 U.S. 696, 703 (1983).

11. Kevin Keener, *Personal Privacy in the Face of Government Use of GPS*, 3 J. L. & POL'Y FOR INFO. SOC'Y 473 (Winter, 2007-2008).

12. *Osburn v. State*, 44 P.3d 523 (Nev. 2002); *State v. Sveum*, 769 N.W. 2d 53 (Wisc. Ct. App. 2009); *United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007); *United States v. McIver*, 186 F.3d 1119 (9th Cir. 1999); *United states v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010).

13. *Commonwealth v. Connolly*, 913 N.E. 2d 356 (Mass. 2009); *People v. Weaver*, 12 N.Y.3d 433 (N.Y. Ct. App. 2009).

14. *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).

15. *Id.* at 563.

16. See *United States v. Jones*, 132 S.Ct. 945 (2012).

17. *Id.* at 951-54.

continuing vitality in this important debate.[18]

This paper examines and analyzes legal cases, Fourth Amendment principles, and legal scholarship relating to how the debate between personal privacy and effective law enforcement has been shaped as technology has evolved. Our aim is to discuss and confront the unique legal and privacy implications that cell site location data tracking through service providers poses for current Fourth Amendment jurisprudence.

Our examination, discussion, and argument will be developed in the following sequence. We first discuss how cell phone tracking works. Next we focus on the legal treatment of the notion of privacy under the Fourth Amendment beginning with the seminal Supreme Court decision of *Katz v. United States*,[19] which laid out the reasonable expectation of privacy test. The discussion also reviews the Supreme Court's historical treatment of tracking devices post-*Katz*. We then review the *Jones* case, the Supreme Court's only decision dealing with GPS tracking of a vehicle. Consideration is directed to the *Maynard* Court's utilization of the "mosaic" theory as a new tool to analyze privacy concerns under the Fourth Amendment, including the implications of *Maynard's* mosaic theory adopted in the two concurring opinions in *Jones* to cell phone user privacy. We conclude by arguing that due to the potentially large amounts of personal information cell phone tracking reveals, the Supreme Court should apply the mosaic theory as a basis of providing cell phone users the protections of the Fourth Amendment.

II. CELL SITE LOCATION TRACKING TECHNOLOGY

To better grasp the debate over cell phone location tracking, it is helpful to have a basic understanding of how cell phone tracking technology works. Unlike traditional land-based lines, cell phones rely on radio waves in order to communicate between the handset and the cellular service network of radio based stations called "cell sites," which are distributed throughout various geographic coverage areas.[20] The quality of the signals to and from the cell sites is typically measured by what most cell phones users understand as the "bars." Whether or not a user is actively engaged in a call, the cell phone will constantly remain in contact with nearby cell towers.[21] The quality and strength of the signals determine through which towers calls are routed both to and from the cell phone in order to provide for the best possible reception and least cross-interference with other cell users.[22]

Importantly, as part of this process, cell phones are constantly conveying

---

18. *Id.* at 955-56, 964.
19. 389 U.S. 347 (1967).
20. *In re* Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 831 (S.D. Tex. 2010).
21. *Id.*
22. Curtiss, *supra* note 8 at 140; Davis, *supra* note 7 at 848.

their location to cell towers in order to have both the strongest signal and to prevent time delays in making and receiving calls. This process of identification, which is referred to as "registration," is automatic and continuously occurs approximately every seven seconds while the phone is on and without any active assistance from the cell phone user.[23] Indeed, the user may be unaware that such information is even being transmitted. The only way to prevent such signals from transmitting is to turn the cell phone off.

Cell site location information is provided to cellular network providers by constant re-registration with whatever cell tower is providing the strongest signal, normally the closest tower.[25] In order to determine which tower is closest to the cell phone, and thereby better route incoming calls in those instances where two towers are both receiving signals from the same phone, provider networks rely on one of two systems to hone in on the phone's location. As a cell phone's location progresses nearer to one tower than another, the nearer tower will recognize increasing strength in the cell phone's signal.[26] The network tower can utilize a Time Distance of Arrival ("TDOA") or Angle of Arrival ("AOA") method, measuring the strength of the signal and thereby the location of the cell phone.[27] A "TDOA" system determines a phone's location by calculating the time it takes a cell phone signal to arrive at multiple cell towers, while "AOA" compares the relative angles from which a cell phone's signal travels to multiple towers, using such information to "triangulate" a cell phone's location.[28]

At the same time, the ability to pinpoint a particular cell phone's location is dependent on the geographical size of the cell sector. The smaller the sector, the more precisely a phone's location can be tracked. Thus, a smaller cell-site allows for more accuracy in determining the user's location.[29] The fact that cell sites have more than tripled in the U.S. over the past 10 years has produced much more accurate tracking information for surveillance activities.[30] If at least three towers that are receiving signals are used in the triangulation process, a nearly precise location of the phone may be determined, perhaps even to a particular floor or room within a building.[31]

The reality is that it is now possible to track an individual using a cell phone within a few meters anywhere on earth. And, of course, one aspect of that reality is the practical utility of this technology for law enforcement surveillance operations. At the same time, there are also more benign, socially beneficial uses of such tracking, such as pinpointing the location of a 911

---

23. *In re* Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 832; McLaughlin, *supra* note 7 at 426; Walsh, *supra* note 6 at 242.

25. Marshall Brain, et al. *How Cell Phones Work,* HOW STUFF WORKS, http://electronics.howstuffworks.com/cell-phone.htm (last visited April 19, 2016).

26. McLaughlin, *supra* note 7 at 426.

27. *Id.*

28. *Id.* at 427.

29. *In re* Application of U.S. for Historical Cell Site Data at 832-33.

30. *Id.*

31. Blaze, *supra* note 1 at 12; McLaughlin, *supra* note 7 at 427.

emergency call from a cell phone, keeping track of where one's children might be, and employers logging the location of mobile employees. As Justice Brandeis once cautioned, experience should be a lesson for each individual to be ready to protect liberty when the government's intentions are "beneficent." [32] However, it is the increasing use of law enforcement tracking of cell site location data that is raising legal and constitutional concerns for privacy advocates, particularly where such tracking is carried out without judicial oversight.[33] Moreover, advanced technologies in the government's hands raise the specter of diminishing the privacy of individuals and current legal paradigms may be unprepared to address this new challenge. [34]

III. RECOGNIZING A REASONABLE EXPECTATION OF PRIVACY

Although the Fourth Amendment does not mention nor make reference to the word "privacy," the Supreme Court has recognized that an individual's Fourth Amendment protections do come into play when that person's "reasonable expectation of privacy" is intruded upon by the government.[35] A "reasonable expectation of privacy" is an expectation that "society is prepared to recognize as reasonable." [36] At the same time, a person cannot expect Fourth Amendment protection in situations where they knowingly expose their activities to the public.[37] Although the Fourth Amendment itself does not textually mandate the inclusion of a "privacy" concept within its scope, it can be maintained that the written text strongly suggests that privacy principles are implicit in its basic terms.

A. *KATZ*: REASONABLE EXPECTATION OF PRIVACY APPROACH

In 1967, the Supreme Court severed its reliance on trespass and property law regarding what constituted constitutionally protected areas. *Katz v. United States* represented a turning point in Fourth Amendment jurisprudence, dramatically shifting the paradigm of Fourth Amendment protections from reliance upon notions of trespass to that of incorporating the concept of privacy into the Fourth Amendment.[38] In rejecting an exclusive reliance on the formalist trespass doctrine, the Court initiated and brought to the fore a new focus from "places" to "people."[39] In *Katz*, the Court confronted the technology of the time. In that instance, the defendant was convicted of transmitting wagering information across state lines by telephone.[40] At trial the Government

32. *Olmstead v. United States*, 277 U.S. 438 (1928)(Brandeis, J., dissenting).
33. *See* Lichtblau, *supra* note 9 at A1.
34. Lawrence Lessig, *Reading the Constitution in Cyberspace,* 45 EMORY L.J. 869 (1996).
35. *See generally Katz v. United States*.
36. *United States v. Jacobsen*, 466 U.S. 109, 122-123 (1984).
37. *Katz* at 361 (Harlan, J., concurring).
38. *Id*. at 353.
39. *Id.*
40. *Id.* at 348.

introduced evidence of the defendant's part of a conversation that was recorded by agents who had attached an electronic recording and listening device to the outside of a public telephone booth.[41] In affirming his conviction, the Court of Appeals, looking to the precedent of *Olmstead v. U.S.*[42] and *Goldman v. U.S.* [43] determined that no Fourth Amendment violation had taken place due to the fact that "there was no physical entrance into the area occupied by [Katz]." [46]

Upon accepting review, the Court first reframed the issues, discarding the trespass and property law basis for determining whether the government had a right to search and seize evidence. As the Court noted, "the premise that property interests control the right of the Government to search and seize has been discredited." [47] Instead, for the first time, the Court recognized that "the Fourth Amendment protects people, not places," [48]and that the protections of the Fourth Amendment "cannot turn upon the presence or absence of a physical intrusion" into a particular area.[49]

Ultimately, the Court held that government monitoring of Katz's telephone conversations from a public phone booth constituted a Fourth Amendment search. As the Court remarked, the government's actions in listening to the defendant's conversation "violated the privacy upon which he justifiably relied while using the telephone booth." [50] The Court went on to note that any similarly situated person who had closed the door in order to place a call would surely be entitled to assume that their conversation was not being overheard.[51]

The Court's majority failed to promulgate any clear test for delineating exactly under what circumstances the Fourth Amendment would "protect people." Nevertheless, it has been Justice Harlan's concurring opinion in *Katz* that has since been regarded as providing the standard regarding what constitutes a "reasonable expectation of privacy." [52] Under Harlan's formulation, there are two requirements that must be met in order to find that a person had a reasonable expectation of privacy: "First, that a person has exhibited an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" [53] For example, Harlan observed that any conduct or words that a person knowingly exposed to the public would not garner protection, even in the privacy of their home.[54] At

41. *Id*.
42. *See generally* 277 U.S. 438.
43 316 U.S. 129 (1942).
46. *Katz* at134.
47. *Id.* at 353 (quoting *Warden v. Hayden*, 387 U.S. 294, 304 (1967)).
48. *Katz* 351.
49. *Id.* at 353.
50. *Id.*
51. *Id.* at 352.
52. *Id.* at 361; *See Smith v. Maryland*, 442 U.S. 735, 740 (1979).
53. *Katz* at 361 (Harlan, J., concurring).
54. *Id.*

the same time, what a person intended to keep as private, even in an area accessible to the public, may create for that individual a reasonable expectation of privacy, as was the case for Katz by his closing the door of the telephone booth.[55] Thus, after *Katz*, a determination of whether government actions constitute a "search" for Fourth Amendment purposes hinges on whether an individual subjectively exhibits an expectation of privacy that society deems reasonable.[56]

It is clear that the burden left for courts applying Harlan's criteria is to examine and consider the place or the information to be protected and the actions taken by an individual to shield that place or information.[57] As one commentator astutely observed a decade prior to the GPS tracking decision of *United States v. Jones*, the critical factor in deciding *Katz* for Harlan was the action taken by the defendant to shield his conversation from being overheard—shutting the phone booth door behind him.[58] What this means for the purpose of this particular endeavor is that courts will be tasked with looking beyond the particular method of surveillance used to the actions of the person being observed or to the information gotten by such surveillance. In the end, applying the *Katz* test may very well come down to making reference to what expectations of privacy our society acknowledges and harbors as being "reasonable."

B. POST-*KATZ*: BEEPER TRACKING AND THERMAL IMAGERS

In order to understand how the reasonable expectation of privacy approach laid out in *Katz* applies to advanced technological surveillance methods, such as GPS and cell site location information tracking, it is necessary to examine some earlier cases involving beeper tracking devices and thermal imaging. The Court's first opportunity to address the issue of tracking devices occurred in the case of *United States v. Knotts.*[59] The Court considered whether enhancement of short-term, visual surveillance by use of an electronic beeper to monitor a chemical container that was being transported by vehicle to a cabin constituted a search for Fourth Amendment purposes. The suspect was tracked both by visual surveillance at the outset and later by monitoring of the beeper signals due to his making "evasive maneuvers." [60] In fact, the beeper tracking became critical after visual surveillance was lost. With the assistance of remote monitoring, the beeper signal was once again picked up and resulted in agents uncovering a drug lab located at the defendant's cabin.[61] The ex-

---

55. *Id*.
56. *United States v. Jones* at 950.
57. Ric Simmons, *From* Katz *to* Kyllo: *A Blueprint for Aadapting the Fourth Amendment to Twenty-First Century Technologies,* 53 HASTINGS L.J. 1303, 1312 (2002).
58. *Id.*
59. *United States v. Knotts*, 460 U.S. 276 (1983).
60. *Id.* at 278.
61. *Id.*

tent of the surveillance was limited to one day.[62]

The Court directed its focus to the question of whether the monitoring of the beeper signals, and thus the defendant's movements, intruded on any legitimate expectation of privacy as delineated in *Katz*.[63] In holding that the monitoring did not encroach upon any "legitimate expectation of privacy" on the defendant's part,[64] the Court noted that there existed a diminished privacy expectation when travelling in a vehicle over a public road, where it was exposed to plain view. As the Court observed, "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." [65] A person, in essence, "voluntarily conveys" their movement and location to any and all observation by others who might be present, including law enforcement.[66] The Court also called attention to the fact that enhancing visual surveillance did not implicate the Fourth Amendment as long as the underlying surveillance did not.[67] Since law enforcement had a legal right to be observing from the public vantage point of a highway, simply enhancing such observation raised no constitutional concern.

One point raised by the defendant will hold some importance in later consideration and analysis of the implications of *United States v. Jones*: the specter of "twenty-four hour surveillance of any citizen" taking place "without judicial knowledge or supervision.[68] In responding to that concern, Justice Rehnquist noted that the amount of such beeper tracking in the case before them hardly suggested abuse.[69] Nevertheless, he did go on to comment that, "if such dragnet-type law enforcement practices… should eventually occur, there will be time enough to determine whether different constitutional principles may be applicable.'' [70] Thus, *Knotts* is only of limited value as precedent in GPS and cell phone tracking cases.

In another beeper case, *United States v. Karo*, the Court nevertheless recognized that under certain circumstances the location information revealed by the tracking device could intrude upon Fourth Amendment protections due to the fact that such information was "not open to visual surveillance." [71] Similar to the facts in *Knotts*, drug enforcement agents attached a beeper to a can of ether and subsequently monitored it as it was being transported by vehicle, ultimately tracing its movement within a private home.[72] Applying the criterion of *Katz*, the Court called attention to the fact that a private home is a place

62. *Id.* at 284-85.
63. *Id.* at 285.
64. *Id.* at 276.
65. *United States v. Knotts,* 460 U.S. at 281.
66. *Id.* at 281-82.
67. *Id*. at 282.
68. *Id.* at 283.
69. *Id.* at 283-84.
70. *Id*. at 284.
71. *United States v. Karo,* 468 U.S. 705, 714 (1984).
72. *Id.*

where a person normally expects to be free from unjustified intrusions by the government, and such an expectation is readily one that society deems justifiable.[73] Addressing the question left unanswered by *Knotts*, the Court observed that when monitoring a tracking device reveals details emanating from the inside of a private home, a protected zone, and which could not have been gotten through visual observation, such tracking constituted a violation of a person's reasonable expectation of privacy.[74]

The Court was later confronted with a more enhanced form of surveillance technology: thermal imaging. In *Kyllo v. United States*,[75] the government utilized a thermal imager to scan the defendant's house from a car located across the street. Suspected of growing marijuana inside his home, the device was used to detect the presence of high-intensity lamps used for such growing, which radiated a relatively high level of heat that was displayed as infrared radiation on the imager. This information formed the basis for securing a search warrant, leading ultimately to the seizure of marijuana.[76]

The government premised its argument upon the notion that the heat emitted from the house was effectively "exposed" to the public.[77] In effect, such a contention would allow a traditionally private space of a person's home to be stripped of any Fourth Amendment protection due to advanced technology "sensing" information from inside the home that would not have otherwise been observable by the public with the naked eye, absent "a physical intrusion into a constitutionally protected" zone.[78] In response to the critical issue raised by the facts in *Kyllo*, that technology poses a threat to privacy by constricting the boundary between public and private in an extreme respect, the Court held that using the imager device under the facts constituted a search and required a warrant.[79]

The Court affirmed the fact that the interior of a person's home is normatively distinct from the exterior, the latter being potentially subject to public view. As in *Katz*, the defendant had a reasonable expectation of privacy in his own home and, "reversing that approach would leave the homeowner at the mercy of advancing technology." [80] Just as Katz had shut the telephone door behind him to keep from being overheard, Kyllo used the walls of his home to cloak from others the temperature of its rooms. [81]

At the same time, the Court included a somewhat cryptic, unexplained methods-based caveat to its sense-enhancing prohibition on collecting infor-

---

73. *Id.*
74. *Id.*
75. 533 U.S. 27 (2001).
76. *Id.* at 27, 29-30.
77. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT, 51 (2007).
78. *Kyllo v. United States* at 34 (quoting *Silverman v. United States*, 365 U.S. 505,512 (1961)).
79. *Kyllo* at 27.
80. *Id.* at 35.
81. J. Harper, *Reforming the Fourth Amendment Privacy Doctrine,* 57 AM. U. L. REV. 1381, 1397 (2008).

mation regarding the interior of the home suggesting that in this case the particular technology was not "in general public use." [86] As one legal commentator has remarked, the Court's inclusion of that language appeared to "drill [...] a technological hole into the walls" of a person's home.[87] It certainly could pose problems where advanced surveillance technologies, such as location tracking devices, become more ubiquitous and widely used by the public. The *Kyllo* Court's opinion certainly was sensitive to the notion that advanced technology holds the negative potential of altering the public, or collective, notion of what constitutes a reasonable expectation of privacy. The decision may portend some significance in determining the scope of Fourth Amendment protections regarding cell site location tracking in suggesting that a constitutional analysis of such tracking not assume methodically and systematically that all information beyond physical boundaries is "public" in nature.

MAYNARD/JONES AND THE RISE OF THE "MOSAIC" THEORY

Despite the ongoing debate in the federal courts as to whether a search warrant based on probable cause, or orders based on lesser standards of proof, are necessary to compel service providers to supply the government with location information, a new conceptual avenue of approaching Fourth Amendment privacy rights in the area of advanced surveillance technologies may be emerging. The "mosaic theory" at its most basic level suggests that as small, discrete bits of information emerge regarding something or some person, at some level those bits of information will yield a picture of that thing or person that is greater than the individual bits themselves. It is the same concept used by the great pointillist painters of the 19th century where the artist would use, instead of brush strokes, thousands of small points of paint that individually were only spots of color but in the aggregate displayed a grand recognizable image.

The mosaic theory is not a recently developed theory, having been raised previously by the government to thwart requests under the Freedom of Information Act in a number of cases where the Supreme Court upheld its use by prohibiting the disclosure of "collective" information. [88] At the same time, its utilization in a Fourth Amendment framework in relation to privacy issues is somewhat unique and newly-minted, having first been applied in the state court GPS tracking case of *People v. Weaver*,[89] where the court found that the continuous monitoring of the defendant over 65 days using a GPS device produced a "highly detailed profile," not only where the defendant travelled, but also by easy inference, his "associations—political, religious, amicable and

86. *Kyllo* at 28.
87. Walsh, *supra* note 6 at 202.
88. *CIA v. Sims,* 471 U.S. 159 (1985); David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act,* 115 YALE L.J. 628, 630 (2005).
89. *See generally People v. Weaver*, 909 N.E.2d 1195 (N.Y. 2009).

amorous." [90] Recognizing the much more sophisticated and powerful nature of the tracking technology used compared to the "very primitive tracking device" employed in the *Knotts* case, the court observed: "[t]hat such a surrogate technological deployment is not …compatible with any reasonable notion of personal privacy or ordered liberty would appear obvious." [91] As reflected in its opinion, the court felt that an expectation of privacy existed beyond the walls of one's home that was consistent with societal views, at least in respect to the quality and quantity of information that could be accumulated by advanced surveillance technologies, and was thus deserving of Fourth Amendment protection.[92]

The *Weaver* court's attention to the "collective" nature of information that can easily be accumulated by the government foreshadows a new road for departing from prior Fourth Amendment jurisprudence as it confronted ever-advancing surveillance technologies.[93] Just as the government seeks to keep private critically valuable collective information it accumulates, so too should individuals be able to assert the mosaic theory in protecting their fundamental right to privacy from continuous monitoring revealing an intimate picture of their life.[94]

The Supreme Court's rather lackluster record on Fourth Amendment privacy issues is perhaps the consequence of its failure to recognize a notion of privacy in a constitutional context that could legally insulate an individual in a public space.[95] Recently, it is the mosaic approach that was utilized and applied in the GPS tracking case of *U.S. v. Maynard*[96] and, was discussed in the more recently re-styled case of *U.S. v. Jones*.[97] The two opinions harbor significant potential for pressing a doctrinal shift in the way Fourth Amendment jurisprudence views an individual's privacy expectation in their continuous and prolonged movements in public space in the face of advancing surveillance technology.

UNITED STATES V. MAYNARD: UNEARTHING THE "MOSAIC" THEORY

A more complete application of the mosaic theory occurred in the D.C. Circuit Court of Appeals case of *U.S. v. Maynard*, where the court embraced the

---

90. *Id*. at 1199.
91. *Id.*
92. *Id.* at 1199-1200.
93. Erin Smith Dennis, *A Mosaic Shield*: Maynard, *the fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737; Madelaine Virginia Ford, Comment, *Mosaic Theory and the Fourth Amendment: How* Jones *Can Save Privacy in the Face of Evolving Technology,* 19 AM.U.J. GENDER SOC.POL'Y & L. 1351 (2011); Susan Friewald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact,* 70 MD. L. REV. 681, 731-45 (2011).
94. *People v. Weaver* at 1199; *United States v. Weaver* at 562.
95. *California v. Ciraolo*, 106 S.Ct. 1809 (1986); *Florida v. Riley*, 488 U.S. 445 (1989); *United States v. Garcia,* 474 F.3d 994; *United States v. Knotts*; *United States v. Pineda-Moreno,* 591 F.3d 1212.
96. *U.S. v. Maynard.*
97. *U.S. v. Jones*.

aggregation principle that the government had put forth in other cases to justify its refusal to reveal information and documents requested pursuant to the Freedom of Information Act.[98] The government's argument has been based on the notion that discrete pieces of seemingly innocuous data can be related to and placed in the context of other isolated pieces of information to reveal a more holistic mosaic, exponentially amplifying each piece's informational value by the picture it constructs, much like a completed jigsaw puzzle.[99]

Maynard dealt with a joint federal and state drug task force, which began investigating Antoine Jones, Lawrence Maynard, and other suspected co-conspirators engaged in cocaine distribution.[100] Agents employed a variety of investigative techniques, including phone taps, visual surveillance, and cell site location information tracking. However, it was not until agents attached a GPS device on Jones' Jeep without a valid warrant and continuously monitored his location information twenty-four hours a day over 28 days that they were able to implicate him in the conspiracy.[101]

Jones' objection to the introduction of the GPS evidence was overruled on the basis that it did not constitute a search due to the fact it did not reveal anything more than he had knowingly exposed to the public by being on the highway, under the rationale of *Knotts.*[102] Jones was convicted, in part, as a result of the GPS data, which revealed a crucial link between him and his co-conspirators. On appeal, Maynard's conviction was affirmed, however, the U.S. Court of Appeals for the D.C. Circuit reversed Jones' conviction on the basis that the long-term, continuous monitoring of Jones by the GPS tracking device over a 28-day period constituted a Fourth Amendment "search."[103]

The court's analysis was divided into separate questions in order to resolve the overriding issue as to whether the sustained monitoring constituted a search. The first inquiry confronted was whether the *Knotts* holding controlled.[104] Judge Ginsburg, writing for the panel, maintained that *Knotts* was not controlling under the facts.[105] The court pointed out that *Knotts* involved short-term surveillance of the defendant over the course of a single trip of approximately 100 miles.[106] In comparison, Judge Ginsburg noted that the scale of surveillance in *Maynard* brought to the fore the very issue explicitly reserved by the *Knotts* Court: whether "dragnet-type law enforcement practices" might implicate "different constitutional principles" than those raised by the tracking of an individual on a single journey.[107] While recognizing that individuals have no reasonable expectation of privacy in discrete, short-term

98. *United States v. Maynard* at 562; *See also CIA v. Sims*.
99. *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1972).
100. *United States v. Maynard* at 549.
101. *Id.* at 555.
102. *See United States v. Knotts*.
103. *United States v. Maynard* at 556-57.
104. *Id*. at 556.
105. *Id*. at 558.
106. *Id.* at 556 (*citing United States v. Knotts* at 277-78).
107. Id. at 556-57 (*citing United States v. Knotts* at 283-84).

travels "from one place to another "on public roadways, which could easily be subject to visual surveillance by police, the *Maynard* Court acknowledged that continuous, prolonged monitoring of an individual's travels by GPS tracking did raise Fourth Amendment issues and that the subject of such surveillance would not necessarily be shorn of a reasonable expectation of privacy in their public travels "whatsoever, world without end." [108]

Freed from the doctrinal limitations of *Knotts*, Judge Ginsburg next directed his inquiry to whether the defendant had, in either an actual or constructive sense, exposed his actions to the public, and to whether an expectation of privacy on his part was reasonable.[109] In order to answer such questions the court referred to *Katz*, observing that: "Whether 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.'" [110] To answer the question of whether the data collected from the GPS tracking was exposed to the public, Judge Ginsburg analytically bifurcated the inquiry into whether someone's conduct had "actually" or "constructively" been exposed to the public.[111]

The government argued that Jones' travels were exposed publically on roads and could have been visually tracked by agents over the course of 28 days.[112] Such a supposition relies on the "potential" [113] or "probability" [114] of law enforcement being able to carry out sustained, traditional visual surveillance in determining "actual exposure." The court's response turned on the distinction between short-term and long-term and to whether observation by the public was an "actual likelihood," as opposed to something potentially possible[115] In essence, the issue of whether to grant a reasonable expectation of privacy in public space hinged upon what a reasonable person expected another individual "might actually do." [116]

Among several Supreme Court cases referenced by Judge Ginsburg, in attempting to flesh out the logic of what a reasonable person would expect other individuals "might actually do," was a case involving a bus passenger who had placed a bag in his overhead storage rack. During a bus stop, police boarded the bus and proceeded to press and squeeze items of luggage with the intent of uncovering drugs, which they ultimately did find in the defendant's bag.[117] In holding that the manipulation of the bag constituted an unwarranted search, the Court pointed to the fact that people do not expect others to

---

108. *United States v. Maynard* at 557.
109. *Id.* at 558.
110. *Id.* (*quoting Katz v. United States* at 351).
111. *Maynard* at 560-61.
112. *Id*. at 559.
113. Walsh, *supra* note 6 at 218.
114. Orin S. Kerr, *Four Models of Fourth Amendment Protection,* 60 STAN. L. REV. 503, 508-511 (2007).
115. *Maynard* at 560.
116. *Id*. at 559.
117. *Bond v. United States*, 529 U.S. 334, 335 (2000); *see Maynard* at 559-60.

handle their personal items with the expectation of finding out what the item contains.

Extending the reasoning of what another is reasonably likely to do to the facts in *Maynard*, Judge Ginsburg determined that even though discrete, isolated pieces of GPS data would be exposed to public view, the entirety of a person's movements over a 28-day period, taken as a collective whole, would not be so exposed due to the fact that it was extremely remote that another person was likely to observe the sum of such movements.[118] Certainly parts of one's travels on a particular day may be observed by others, but as Judge Ginsburg pointed out:

> A reasonable person does not 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.[119]

Thus, due to the fact that it was highly unlikely that the public could have observed the sum of the defendant's movements, the court determined that those movements could not be described as having been "actually exposed" to the public's view.[120]

Perhaps the most significant aspect of Ginsburg's treatment of privacy in public space is in his utilization of what had previously been used by the government as a prophylactic against divulging "private" information—the mosaic theory. His adaptation of the theory to Fourth Amendment jurisprudence allowed the court to shift the attention to the quantity and quality of the information acquired by the government, as opposed to discrete, isolated movements as the critical factor in these cases.[121] In this new theoretical approach to the issue of privacy in public space, Judge Ginsburg maintained that even if a person's discrete, isolated movements were "constructively exposed" to the public—that is, exposed regardless of having actually been seen—the aggregation of information collected over a 28-day surveillance period was not constructively exposed due to the fact that the nature of the information was qualitatively different and more revealing than its disparate parts.[122] In essence, "[t]he difference is not one of degree, but of kind," revealing "an intimate picture of [one's] life." [123] Pieces of information data might seem innocuous in themselves, isolated from one another. However, assembled together into a mosaic, they assume a qualitatively different and more revealing character than the disparate facts that make up the whole. Finding that the continuous and sustained surveillance by GPS tracking exposed an intimate picture of Jones' life that was reasonable for him to keep private, the *Maynard* Court overturned Jones' conviction.

---

118. *Maynard* at 558.
119. *Id.* at 563.
120. *Id.*
121. *Id*. at 562.
122. *Id.* at 561-62.
123. *Id*. at 562.

UNITED STATES V. JONES: ENDORSEMENT OF THE MOSAIC THEORY

On appeal, the Supreme Court unanimously, although split on the rationale, agreed with the D. C. Circuit's holding that Jones' Fourth Amendment rights had been violated, but did so on a much narrower basis than did the *Maynard* court.[124] The majority opinion, written by Justice Scalia, held that the attachment of the GPS tracking device to Jones' vehicle for the purpose of monitoring him constituted a search when the government trespassed upon the vehicle, which is protected by the Fourth Amendment as an "effect." [125] As a consequence of the trespass, Justice Scalia found no need to apply the *Katz* formulation in resolving the case. Instead, he viewed the expectation of privacy test as supplemental to the common-law trespass test.[126] Having avoided the issue of applying the analytical framework of *Katz*, the majority deferred the issue of whether long-term, continuous surveillance constitutes a search, as the *Maynard* court had found by employing the mosaic theory. As Justice Scalia observed, the Court might have to deal with problematic issues in the future with a search case involving no trespass and have to employ the *Katz* test: "but there is no reason for rushing forward to resolve them here." [127]

Five justices, however, were willing to forge ahead on the same analytical tracks as Judge Ginsburg laid down in *Maynard*. Justice Alito's concurring opinion, joined by three other justices, focuses on the issue of whether "the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated." [128] His concern is that applying a trespass rule might allow for advanced technology to monitor an individual without any technical trespass and allow the surveillance to continue for an indefinite period of time absent judicial oversight and review, which would contravene the public's reasonable privacy expectations. The public, in Justice Alito's opinion, does not expect their every movement to be secretly monitored over a long period of time, such as the 28 days in Jones' case.[129] Under Alito's analytical structure there is a distinction between "relatively short-term monitoring of a person's movements" in public and long-term, continuous surveillance like that in *Jones*, the latter being a search while the former may or may not be.[130] The basis of the distinction resonates from the *Katz* decision itself: what would society regard as a reasonable expectation of privacy?

Justice Alito's concern over the distinction between short-term and long-term monitoring is central to the mosaic approach. The longer and more continuous the monitoring, the more probable and likely that a larger number of discrete, isolated data points can be associated and interrelated into a collec-

124. *United States v. Jones* at 948.
125. *Id.* at 949.
126. *Id*. at 952.
127. *Id.* at 954.
128. *Id*. at 964 (Alito, J., concurring).
129. *Id*.
130. *United States v. Jones.*

tive mosaic; in relation to privacy, "the whole may be more revealing than the parts." [131] The end result of advanced surveillance technologies is that they allow for the collection of information that is of a qualitatively different character: unanticipated, subject to being abused, and perhaps, inimical to society's notions of what constitutes a free society.

Justice Sotomayor, in a concurring opinion, expressed similar concerns. Initially, she agrees with the majority opinion that held a search had taken place where the government had physically encroached on a constitutionally protected area, Jones' vehicle, without a valid warrant and without Jones' consent.[132] However, after supporting the trespass principle as a sufficient basis for deciding the case, describing it as an "irreducible constitutional minimum,"[133] she goes on to develop perhaps the most unrestrained and far-reaching notion of privacy of all the justices.

Justice Sotomayor not only subscribes to Justice Alito's position that long-term surveillance encroaches on expectations of privacy, but has additional concerns. Even short-term monitoring she suggests might require more focused attention in instances where advanced technology is employed that generates more precise and comprehensive records of an individual's movements, evidencing "a wealth of detail about her familial, political, professional, religious, and sexual associations."[134] Other concerns of hers relate to the inexpensiveness of such technologies, compared to traditional surveillance methods and, the secrecy in its application, evading judicial oversight that might restrict abuse by those engaged in it.[135]

Justice Sotomayor's opinion reflects an instinctive distrust of power, and the misuse of it by those who hold it; that the misemployment of highly invasive technologies stands opposed to an open and democratic society with its potential to "chill" protected freedoms and to alter the relationship between citizen and state.[136] The concerns Justice Sotomayor brings into the privacy debate are anchored in a normative paradigm that inquires whether individuals reasonably expect that their every movement will be aggregated and stored in a way that reveals an entire picture, or mosaic, of who they are, what they do, who they associate with, and where they go, both in public and in private.

SHAPING THE FUTURE DEBATE ON PRIVACY EXPECTATIONS

Privacy is a concept that is susceptible to more expansive or more restrictive meanings, depending on societal attitudes often formed in the face of technological advances. As privacy scholar Christopher Slobogin has re-

131. *Maynard* at 561.
132. *Jones* at 954 (Sotomayor, J., concurring).
133. *Id.* at 954-55.
134. *Id*. at 955.
135. *Id.*
136. *Id*. at 956.

marked: "privacy is a very elastic animal." [137] Similar to many provisions in the Bill of Rights, such as freedom of speech and association, and the prohibition on cruel and unusual punishment, the Fourth Amendment was drafted in part based on the Framers' reaction to the centralized power latent in a strong federal government.[138] The text of the Fourth Amendment evidences a purpose to protect freedom and dignity against the exercise of intrusive and abusive governmental actions distinctive of a surveillance state: erecting "a wall between a free society and overzealous police action . . . to protect individuals from the tyranny of the police state." [139] Indeed, the Supreme Court has recognized that the Constitution was set up to place barriers in the way of "permeating police surveillance," which was viewed with more disdain than allowing criminals to escape from punishment.[140]

The same apprehension experienced by the early Framers, and reflected in past Supreme Court comments, exists in the present day as law enforcement expands its access and use of advanced surveillance capabilities in a more pervasive and intrusive monitoring of citizens. The determination to be made in regard to cell site location tracking by police is how this new mode of surveillance fits into the Court's Fourth Amendment jurisprudence. At its most basic formulation is whether the government can access cell site location data for continuous monitoring of individuals without Fourth Amendment constraints. As one privacy scholar has remarked: "[t]he answer must be 'no.'" [141]

All nine justices in *Jones* conceded that technological surveillance in the absence of any trespass could transgress the Fourth Amendment under the reasonable expectation of privacy formulation expounded by Justice Harlan in *Katz.* As the majority opined, "mere visual surveillance does not constitute a search, however, "[it] may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy."[142]

Justice Alito's opinion focuses squarely on the constitutional issue although his analysis and its application is treated in abstract terms, lacking a clear delineation as to when a particular monitoring operation has gone over the line to becoming a "search." [143] Justice Sotomayor's opinion, on the other hand, solidly grounds her analysis in referents to individual liberties and freedoms by arguing that GPS tracking and, by extension, cell site location tracking portend detrimental consequences for a democratic society.[144] She con-

---

137. Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory,* 8 DUKE J. CONST. L. & PUB. POL'Y 1, 11 (2012).

138. *See* Anthony Amsterdam, *Perspectives on the Fourth Amendment,* 58 MINN. L. REV. 349 (1974).

139. Renee Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment,* U.C.L.A. L. REV. 409, 444 (2007).

140. *United States v. Di Re*, 332 U.S. 581, 595 (1948).

141. Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact,* 70 MICH. L. REV. 681, 745 (2011).

142. *Jones* at 953-54.

143. *Id.* at 964 (Alito, J., concurring).

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

tends that such long term tracking can chill "associational and expressive freedoms," ultimately giving way to a change in the relationship between citizen and state in a manner she views as "inimical to democratic society." [145] Her resolution of whether non-trespassory monitoring constitutes a search would be dependent on an objective reference to societal normative expectations, inquiring: "[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."[146] Although Justice Sotomayor never explicitly uses the term "mosaic" to describe her analytical approach to such tracking, it is evident that her design and that of the *Maynard* Court are doctrinally alike.

The *Maynard* decision and the two concurring opinions in *Jones* hold the potential of re-galvanizing Fourth Amendment protections in an advanced surveillance age of cell site location data tracking. Given the omnipresence of cell phones and the fact that such tracking by the government provides an intimate and comprehensive view of individuals' private lives, it is incumbent for courts to look to the Fourth Amendment's provisions regarding probable cause and warrants for guidance.

The *Maynard* Court's approach, along with the reasoning of Justices Sotomayor and Alito in *Jones*, evidences significant potential for reshaping and adapting the boundaries of Fourth Amendment jurisprudence regarding advanced surveillance technologies in an information age. The mosaic construct presents a strong bulwark for privacy protection in the face of increasingly more intrusive monitoring capabilities exploited by law enforcement, particularly in regard to personal information accumulated by third-party automated intermediaries like cell phone service providers. As one commentator has correctly observed, the present approach taken by law enforcement to electronic information harkens back to the early Founders' days where writs of general assistance authorized the indiscriminant accumulation of information on colonists without warrants based on probable cause.[147] The false categorization that individuals "voluntarily" disclose to automated third-party intermediaries vast amounts of personal information directly confronts "an expectation of privacy that our society recognizes as reasonable.[148]

The government continues to rely on the Supreme Court opinions of *United States v. Miller*[149] and *Smith v. Maryland,*[150] arguing that cell phone users lack any reasonable expectation of privacy in historical cell site information due to the fact that users voluntarily expose such information to a third party, in this case the cell phone provider.[151] This rather antiquated ra-

145. *Id.*
146. *Id*.
147. John P. Collins, *The Third Party Doctrine in the Digital Age* (2012), *available at* www.nyls.edu/capstones.
148. *Maynard* at 556.
149. 425 U.S. 435 (1976).
150. 442 U.S. 735 (1979).
151. *United States v. Miller* at 442; *Smith v. Maryland* at 742-44.

tionale, the "third –party doctrine," holds that cell phone users should be aware that they are sending information about their location to the phone provider and thus lack any reasonable expectation in such "volunteered" information. However, as Justice Sotomayor remarked in *Jones,* the third-party doctrine is "ill suited to the digital age," where individuals expose a great amount of information concerning themselves to third parties.[153] Unrealistically, in our technological era, a person's only option of preventing the collection of cell site location information would be to not own a cell phone.

Nevertheless, the winds of change may be blowing. The Supreme Court's recent decision in *Riley v. California,* where the court specifically made reference to Justice Sotomayor's concurring opinion in *Jones*, rejected application of the third-party doctrine to the search of a cell phone incident to an arrest.[154] In limiting the searches of cell phones incident to arrest, the Courted noted that such searches are "qualitatively different" than searches of physical evidence,[155] and the implications far greater for privacy interests.[156]

The federal courts are divided on the issue of police accessing cell site location data by the government without a search warrant. In 2013 the Fifth Circuit found there was no expectation of privacy in historical cell site location data.[157] In June of 2014, the Eleventh Circuit Court of Appeals reached the opposite conclusion in becoming the first federal appeals court to recognize a privacy expectation in cell site location information, requiring law enforcement to obtain a search warrant for such.[158] In following the lead of the Supreme Court in the *Jones* case, the Eleventh Circuit panel clearly relied on the reasonable expectation of privacy test regarding the government's acquisition of location information, specifically cognizant of the fact that the *Jones* Court clearly retained the test from *Katz*.[158] At the same time, while the *Jones* Court was overtly concerned about the potential for governmental abuse of aggregated information data, the *Davis* court went further in holding that even a single point of cell site location information, such as a visit to a psychiatrist, could come within a reasonable expectation of privacy.[159] Thus, a privacy interest could attach long before any "mosaic" had been created.[160]

CONCLUSION

Cell site location information tracking poses a threat to privacy in ways

153. *Jones* at 957 (Sotomayor, J., concurring).
154. 134 S. Ct. 2473.
155. *Id.* at 2490 (*citing* Jones at 955)(Sotomayor. J., concurring).
156. *Id. at* 2491.
157. *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).
158. *U.S. v. Davis*, 754 F.3d 1205, 1217 (11th Cir. 2014) reh'g en banc granted, opinion vacated, 573 Fed. Appx. 925 (11th Cir. 2014)(unpublished) and on reh'g en banc in part, 785 F.3d 498 (11th Cir. 2015) cert. denied, 136 S. Ct. 479 (2015).
158. *Katz* at 361.
159. *United States v. Davis*.
160. *See* Freiwald, *supra* note 141 at 748-49.

that traditional tracking of a suspect using beepers could not. The more efficient and cost-effective monitoring using CSLI allows for continuous and sustained intrusion into private matters. As the *Maynard* Court pointed out, GPS and, by extension CSLI tracking, bring to the fore a completely different and "unknown type of intrusion into . . . ordinarily and hitherto private enclave[s]."[161] As privacy advocate Daniel Solove has written, the information accumulated can reveal an intimate portrait of who we are, in essence, our identities.[162] The wealth of such information creates a virtual map of an individual's movements that has never been available to law enforcement to such a degree and quality and that goes far beyond call-identifying data. Compared to the GPS tracking in *Maynard/Jones*, CSLI reveals more about a person due to the fact that people carry their cell phones wherever they go: in purses and pockets, to the doctor's office, to a political gathering, in their own home, and even inside their bedroom.

The fact that cell phones are carried into places – "withdrawn from public view"- where individuals have a reasonable expectation of privacy, clearly raises Fourth Amendment concerns as *U.S. v. Karo* recognized.[163] Even if a cell phone owner makes no calls, the phone's presence inside the home will be disclosed by the automatic registration process,[164] thus raising serious Fourth Amendment concerns.

Long-term, continuous monitoring of cell site location information taking place in public space would fall squarely within the contours of the mosaic theory of the Fourth Amendment, recognizing that "when it comes to privacy . . . the whole may be more revealing than the parts."[165] Reflecting Judge Ginsburg's analytical approach in *Maynard*, Justice Alito directs focus to the question as to what society would reasonably expect. His observation is that society would not expect police, or others, to covertly monitor a person's every movement for long periods of time.[166] The qualitative distinction presented by CSLI tracking simply will not be anticipated by individuals in a free society.[167] In that event, cell site location tracking would certainly call for Fourth Amendment protection.

At the same time, Justice Sotomayor's opinion offers a forceful directive, squarely situated within the early Framers' own distrust of government power and analytically grounded in other constitutional freedoms, such as the freedom of expression, religion and association.[168] Her message is that power is susceptible to being abused; the end product of such abuse may be to "chill associational and expressive freedoms." [169] Other legal scholars have voiced

---

161. *Maynard* at 565.
162. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY, 33 (2008).
163. *United States v. Karo,* 468 U.S. at 716.
164. *In re* Application of U.S. for Historical Cell Site Data at 836.
165. *Maynard* at 561.
166. *Jones* at 964 (Alito, J., concurring).
167. *Id.*
168. *Id.* at 956 (Sotomayor, J., concurring).
169. *Id.*

similar concerns.[170] Importantly, she calls attention to the fact that such "chilling" may alter the power "relationship between citizen and government" in a manner "that is inimical to democratic society." [171]

Embodied in her perspective is the view that a surveillance state is undemocratic and not fully free without a notion of privacy that fosters the engagement of citizens in a self-directed public life, which is crucial to the reality of public citizenship in a democracy. Justice Douglas conveyed like sentiments some 40 years earlier:

> [C]oncepts of privacy which the Founders enshrined in the Fourth Amendment vanish completely when we slavishly allow an all-powerful government, proclaiming law and order, efficiency, and other benign purposes, to penetrate all the walls and doors that men need to shield them from the pressures of a turbulent life around them and give them the health and strength to carry on.[172]

It is evident that Justice Sotomayor believes that in order for a democracy to thrive in a meaningful way that individuals need to be free of undue and intrusive surveillance that can inhibit the development of meaningful social discourse, debate, and individual personal growth and autonomy necessary to fostering a citizenship capable of applying their conception of how best "to live their own lives." In short, she clearly intimates that indiscriminate, long-term monitoring of citizens can place into jeopardy the purpose and design of democratic society, which is the free, unintimidated citizen involvement in the life of the community.

The challenge facing the Court is to interpret and apply Fourth Amendment principles as originally conceived by the Framers to ever-evolving technologies of surveillance; to refer to the principles that the Amendment inherently implies and to find in those principles the tools to address how government will collect information about citizens in a democratic and open society. This present endeavor maintains that the mosaic theory provides the most compelling approach to addressing the challenge.

---

170. Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the right to Anaonymity,* 72 MISS. L.J. 213, 253-55 (2002); Daniel J. Solove, *The First Amendment as Criminal Procedure,* 82 N.Y.U. L. REV. 112, 143-44 (2007).

171. *Jones* at 956 (Sotomayor, J., concurring).

172. *United States v. White*, 401 U.S. 745 (1971) (Douglas, J., dissenting).