Nebraska Law Review

Volume 92 | Issue 3 Article 3

2014

District of Columbia *Jones* and the Mosaic Theory—In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory

Jace C. Gatewood
John Marshall Law School, Atlanta, jgatewood@johnmarshall.edu

Jace C. Gatewood*

District of Columbia *Jones* and the Mosaic Theory—In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory

TABLE OF CONTENTS

* Jace C. Gatewood (Georgetown University, A.B., 1983; Georgetown University Law Center, J.D., 1990), Associate Professor of Law at Atlanta's John Marshall Law School. I would like to express my deepest gratitude and thanks to my research assistant, Ms. Kandice Allen, whose thorough research and tireless dedication were invaluable to the completion of this Article.

I. INTRODUCTION

If you are a diehard fan, as I am, of the famed Indiana Jones movie franchise,[1] you will undoubtedly remember Indiana Jones and the Last Crusade.[2] In this third installment of the Indiana Jones franchise, Indiana Jones, the renowned adventurer and archaeologist, receives a diary from his father, Dr. Henry Jones Sr., that holds several innocuous clues and a map with no monikers that supposedly reveals the location of the wondrous Holy Grail.[3] By piecing together seemingly innocuous clues, one after another, clue by clue, using only the diary and the map as a guide, Indiana Jones is able to determine the exact location and whereabouts of the Holy Grail, which had been mysteriously lost for hundreds of years, and, in doing so, he managed to stop Adolf Hitler and the Nazis from world domination. Imagine, taking ostensibly independent, innocuous clues that hold very little probative value in and of themselves but, when amassed together, hold the secret to the greatest discovery of mankind: a secret that for several hundred years the Knights of the First Crusade defended, died for, and tried to keep hidden from public eye. Well, while only a fictional movie, this is exactly what Indiana Jones was able to do in 1938 using only a diary and a map with no names. Imagine the movie today, but only this time, Indiana Jones has a GPS device.[4]

Essentially, but in less dramatic form, this is the argument raised by District of Columbia Jones[5] in *United States v. Maynard*.[6] Antoine Jones, who was the owner of a nightclub in the District of Columbia called "Levels," was convicted of conspiracy to distribute and possession with the intent to distribute cocaine and cocaine base.[7] Jones's

1. The Indiana Jones movie series was created by George Lucas and directed by Stephen Spielberg and included four installments: Raiders of the Lost Ark in 1981, Indiana Jones and the Temple of Doom in 1984, Indiana Jones and the Last Crusade in 1989, and Indiana Jones and the Kingdom of the Crystal Skull in 2008.
2. *Id.* The Indiana Jones and the Last Crusade screenplay was written by Jeffrey Boam.
3. The Holy Grail is most commonly identified with a cup or chalice used by Jesus Christ at the Last Supper. *See* definition of "grail," MERRIAM-WEBSTER DICTIONARY (2013).
4. A GPS is a device that receives Global Positioning System (GPS) signals capable of determining a user's exact location anywhere in the world. *See* Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 414–21 (2007) (detailing the science and uses of GPS technology).
5. "District Columbia Jones" is a metaphoric reference to the defendant, Antoine Jones, the District of Columbia nightclub owner whose conviction for drug conspiracy was overturned in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom*. United States v. Jones, 132 S. Ct. 945 (2012).
6. 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom*. United States v. Jones, 132 S. Ct. 945 (2012).
7. *Id.* at 548–49.

conviction was based in part on the use of a GPS tracking device attached to a Jeep driven by Jones. The GPS tracking device was used by law enforcement to track Jones's movements twenty-four hours a day over a twenty-eight day period.[8] Jones argued that his conviction should be overturned because the police violated his Fourth Amendment rights by tracking him without a warrant.[9] Specifically, Jones argued that the use of the GPS tracking device violated his "reasonable expectation of privacy"[10] and was therefore a search under the Fourth Amendment. The D.C. Circuit Court, in an opinion written by Judge Douglas Ginsburg and joined by Judges Tatel and Griffith, decided that the government's warrantless use of a GPS tracking device to track Jones's every movement for a four-week period violated his Fourth Amendment protection against unreasonable searches and introduced a new theory of Fourth Amendment jurisprudence—the "mosaic theory."[11]

The mosaic theory refers to a concept borrowed from a series of cases involving challenges by the government to requests under the Freedom of Information Act (FOIA),[12] which was adapted by the *Maynard* court for Fourth Amendment use.[13] The theory is based on the concepts that the whole is greater than the sum of its individual parts and that the aggregation of information takes on greater significance when combined with other information.[14] "Combining the items illuminates their interrelationships and breeds analytic synergies, so that the resulting mosaic of information is worth more than the sum of its parts."[15] Applying this theory in *Maynard*, the D.C. Circuit Court found that isolated and discrete actions of the government that are not deemed searches individually may become searches when aggregated together en masse,[16] thus violating a person's reasonable expectation

8. *Id.* at 555.
9. *Id.*
10. *See generally* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
11. *See generally* David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005) (discussing the evolution of the mosaic theory in the context of the FOIA and national security).
12. *See id.*
13. *See Maynard*, 615 F.3d at 560–63.
14. *See* Pozen, *supra* note 11, at 630. *See also Maynard*, 615 F.3d at 561 (discussing prior courts' distinctions between the whole and the sum of its parts in regard to data collection).
15. Pozen, *supra* note 11, at 630.
16. See *Maynard*, 615 F.3d at 558. In rejecting the government's contention that no distinction should be drawn between the information discovered by use of a beeper in a single discrete journey at issue in *Knotts* and the more comprehensive monitoring at issue in *Maynard*, the Circuit Court applied the mosaic theory, stating that:

> [T]he totality of Jones's movements over the course of a month—was not exposed to the public: First, unlike one's movements during a single

of privacy.[17] Aided by this newly formulated theory, the *Maynard* court found that the government's warrantless use of a GPS tracking device to track the defendant's public movements for four weeks violated the defendant's reasonable expectation of privacy and constituted a search under the Fourth Amendment.[18]

The *Maynard* decision marked a dramatic shift in Fourth Amendment jurisprudence and, at the time of its decision in 2010, was contrary to holdings of several other circuit courts.[19] When the Supreme Court reviewed the *Maynard* decision in 2012 in the retitled action *United States v. Jones*,[20] even though the Supreme Court did not resolve the case using the mosaic theory, Justice Sotomayor's concurring opinion and Justice Alito's concurring opinion, which was signed or joined by three other justices, endorsed some form of the mosaic theory.[21]

> journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil. Second, the whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts.

Id.

17. *See id.*
18. *See Maynard*, 615 F.3d at 563 ("Society recognizes Jones's expectation of privacy in his movements over the course of a month as reasonable, and the use of the GPS device to monitor those movements defeated that reasonable expectation.").
19. *See, e.g*., United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010) (holding that despite a lack of standing, defendant's Fourth Amendment rights were not violated by installation and use of a GPS tracking device on defendant's vehicle); United States v. Pineda-Moreno, 591 F.3d 1212, 1215 (9th Cir. 2010) (holding that the use of GPS tracking device did not violate the Fourth Amendment rights of defendant because defendant had no reasonable expectation of privacy), *cert. granted*, 132 S. Ct. 1533 (2012); United States v. Garcia, 474 F.3d 994, 997–98 (7th Cir. 2007) (holding that the warrantless use of GPS tracking device on defendant's vehicle was not a search or seizure).
20. 132 S. Ct. 945 (2012).
21. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012) ("The majority opinion resolved the case without reaching the mosaic theory, and neither concurring opinion gave the issue extensive analysis. But Justice Alito's concurring opinion for four [J]ustices clearly echoed the basic reasoning of the D.C. Circuit in concluding that long-term GPS monitoring of a car counts as a search even though short-term monitoring does not. Justice Sotomayor's separate concurrence also voiced support for the mosaic approach.") (footnotes omitted). *See also Jones*, 132 S. Ct. at 955–56 (Sotomayor, J., concurring). Concerned about the degree of intrusiveness capable with GPS technology, Justice Sotomayor questioned "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the [g]overnment to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." *Id.* at 956. Justice Alito also seems to be in accord with Justice Sotomayor when he states, "for four weeks, law enforcement agents *tracked every movement* that respondent made in the vehicle he was driving." *Id.* at 964 (Alito, J., concurring in judgment) (emphasis added).

In the aftermath of *Maynard*, many articles were written on the mosaic theory and its viability for Fourth Amendment application.[22] Some of the articles argued against the wisdom of the mosaic theory and its use in Fourth Amendment jurisprudence because of its impracticability.[23] According to those commentators, implementing the mosaic theory would be difficult if not impossible to administer.[24] Without a doubt, the mosaic theory raises several challenging issues for the future of Fourth Amendment jurisprudence. Notwithstanding, however, and despite the wide-ranging criticism, the application of the mosaic theory may help establish and restore a balance between our public and private lives.

Prior to the dawn of modern technology, "the greatest protections of privacy were neither constitutional nor statutory, but practical."[25] In the pre-computer age, we could go about our daily public lives without the fear or even conscious thought that our day-to-day movements and our comings and goings were monitored or even taken note of, precisely because the effort and cost required to undertake such a task was impractical.[26] Today, amid new technologies capable of constant twenty-hour, seven-day-a-week monitoring, the boundary between our public and private life is no longer defined by practical considerations and, as a result, our privacy (and our reasonable expectation of privacy) is being eroded with each new technological advance. With to-

22. *See, e.g.*, Kerr *supra* note 21; 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 (2012); 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); Benjamin M. Ostrander, Note, *The "Mosaic Theory" and Fourth Amendment Law*, 86 NOTRE DAME L. REV. 1733 (2011); Bethany L. Dickman, Note, *Untying Knotts: The Application of Mosaic Theory to GPS Surveillance in* United States v. Maynard, 60 AM. U. L. REV. 731 (2011); Erin Smith Dennis, Note, *A Mosaic Shield:* Maynard*, The Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737, 739 (2011).

23. *See, e.g.*, Kerr, *supra* note 21, at 346 ("The first difficulty with the mosaic theory is the most obvious: its implementation raises so many difficult questions that it will prove exceedingly hard to administer effectively."); Ostrander, *supra* note 22, at 1748 ("The application of the 'mosaic theory' to the Fourth Amendment would not only be wrong in principle, it would be impractical in application."). *But see* Ford, *supra* note 22, at 1365 ("The mosaic theory is a novel theory in the Fourth Amendment context and it could dramatically change privacy jurisprudence."); Dennis, *supra* note 22, at 739 ("The mosaic theory of privacy proffered in *Maynard* has the potential to impact not only GPS surveillance, but the wider realm of Internet and digital surveillance . . . ."); Dickman, *supra* note 22, at 737–38 ("The mosaic theory is a novel and much-needed addition to the traditional Katz framework.").

24. *See* Kerr, *supra* note 21, at 346.

25. *Jones*, 132 S. Ct. at 963 (Alito, J., concurring in judgment).

26. *See id.* at 963 (Justice Alito noted, "Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken.").

day's technology, the government is no longer constrained by investigatory methods that require massive amounts of time, manpower, or resources.[27] New technology has enabled law enforcement officials to become more cost-effective and efficient, without concern with the practical considerations that existed prior to wiretaps,[28] pen registries,[29] thermal scanners,[30] beepers,[31] and GPS technology.[32]

Notwithstanding the many issues raised with respect to the use of the mosaic theory as a new Fourth Amendment theory for protection of privacy rights,[33] the application of the mosaic theory in Fourth Amendment jurisprudence may help resolve issues that neither *Katz* nor *Jones* resolve[34] and may help strike a balance between the government's interest in investigating crime and society's interest in maintaining privacy in and out of the public eye. In short, the mosaic theory will ensure the degree of public privacy, particularly with respect to our public movements, that society has come to expect, despite the erosion of practical considerations that once limited the extent to which law enforcement could invade individual privacy rights without violating the Fourth Amendment.[35]

In this regard, this Article will discuss the mosaic theory and the issues raised regarding its viability in resolving Fourth Amendment privacy concerns, particularly concerns raised over one's public movements from place to place in the wake of advanced surveillance and monitoring technology. Additionally, this Article will discuss how application of the mosaic theory, despite its flaws, may provide a balanc-

27. *See id.* at 963–64. Referring to the GPS surveillance at issue in *Jones*, Justice Alito noted that if traditional methods of surveillance were employed to monitor the defendant for four weeks "a large team of agents, multiple vehicles, and perhaps aerial assistance" would have been required. *Id.* at 963. Justice Alito also noted that devices like the one at issue in *Jones*, "make long-term monitoring relatively easy and cheap." *Id.* at 964.

28. *See generally* Olmstead v. United States, 277 U.S. 438 (1928); Goldman v. United States, 316 U.S. 129 (1942).

29. *See generally* Smith v. Maryland, 442 U.S. 735 (1979).

30. *See generally* Kyllo v. United States, 533 U.S. 27 (2001).

31. *See generally* United States v. Knotts, 460 U.S. 276 (1983); United States v. Karo, 468 U.S. 705 (1984).

32. *See generally Jones*, 132 S. Ct. 945 (2012).

33. *See supra* note 23 and accompanying text. *See also infra* section III.C (addressing concerns regarding the implementation of mosaic theory).

34. *See* Jace C. Gatewood, *It's Raining* Katz *and* Jones*: The Implications of* United States v. Jones*—A Case of Sound and Fury*, 33 PACE L. REV. 683 (2013) (making the argument that neither *Katz* nor *Jones* provides adequate protection against warrantless surveillance either because, given today's technology, there is no physical trespass involved, because of the nature of the intrusion involved, or because of the pervasiveness of the technology involved).

35. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring in judgment) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

ing effect between the protections afforded by the Fourth Amendment and technological advances that continually blur the line between what is private and what is public, skewing the scope and meaning of the Fourth Amendment.

To address these issues, this Article is divided into three parts. Part II of this Article focuses on how advances in technology have recurrently exerted pressure on the Fourth Amendment, eroding practical limitations and creating a ridged line between that which is private and that which is public. Part III discusses the mosaic theory, its application in *Maynard* and *Jones*, and the issues raised with respect to its possible future application in Fourth Amendment jurisprudence. Finally, Part IV argues that despite all of the concerns and issues raised with respect to the future application of the mosaic theory, the mosaic theory offers a unique opportunity for the Court to reestablish equilibrium among the competing values of privacy and surveillance, fashioning what might be called a public right of privacy.

II. TECHNOLOGY AND THE FOURTH AMENDMENT

A. Original Intent of the Fourth Amendment and Its Practical Limitations

The Fourth Amendment states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[36] This proscription has broadly been interpreted to include a right of privacy[37]—the right to be free from unreasonable governmental interference. Unfortunately, the privacy protection thought to be guaranteed by the Fourth Amendment has never been well-defined.[38] As a consequence, the fundamental protections offered by the Fourth Amendment have become increasingly blurred by the high-tech advances of the past century.[39]

When the Framers adopted the Fourth Amendment in 1791, the search and seizure issues confronted by today's Supreme Court could have never been imagined given the technological realities of the

36. U.S. CONST. amend IV.

37. *See* Jace C. Gatewood, *Warrantless GPS Surveillance: Search and Seizure—Using the Right to Exclude to Address the Constitutionality of GPS Tracking Systems Under the Fourth Amendment*, 42 U. MEM. L. REV. 303, 363–65 (2011) (discussing the shift from a property-based paradigm to a privacy-based paradigm under the Fourth Amendment).

38. *See* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67 (discussing the history of Fourth Amendment search doctrine from its original understanding, to its understanding before *Olmstead* in 1928, to its understanding from *Olmstead* to *Katz* and concluding that the commonly accepted definition of the term "search" has been misunderstood).

39. *See* Tracey Maclin, Katz*,* Kyllo*, and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 51–58 (2002).

eighteenth century.[40] During the Framers' era, the focal point of privacy was the home.[41] Evidence suggests that "[s]earches [under the Fourth Amendment] referred to the forcing open of persons' houses and the breaking open of their desks and cabinets in an effort to find the evidence inside."[42] Thus, as a practical matter, in order to violate the proscriptions of the Fourth Amendment during the Framers' era, and much of the time leading up to the Supreme Court's most recent decision in *United States v. Jones*,[43] there needed to be some sort of physical entry or trespass by the government.[44] The use of trespass as the predominate theory to determine Fourth Amendment violations is evident throughout the Fourth Amendment's doctrinal history.[45] The Supreme Court's decision in *Jones* strongly supports this view.[46] Thus, it's clear that throughout our history, the law of trespass imposed a practical limitation on the government's right to intrude into our private lives.[47] Not only did the law of trespass impose a practical

40. *Id.* at 52. *See also Jones*, 132 S. Ct. at 958 (2012) (Alito, J., concurring in judgment) (referring to the use of GPS technology and the application of eighteenth century tort law to GPS use, Justice Alito comments that "it is almost impossible to think of late-18th-century situations that are analogous to what took place in this case").

41. *See* Kerr, *supra* note 38, at 72 ("Famous search and seizure cases leading up to the Fourth Amendment involved physical entries into homes, violent rummaging for incriminating items once inside, and then arrests and the taking away of evidence found. These examples, and some contemporaneous statements during the ratification debates, suggest that home entries and rummaging around inside were understood as the paradigmatic examples of 'searches.'").

42. *Id.* at 7.

43. 132 S. Ct. 945 (2012).

44. *See* Kerr, *supra* note 38, at 73–74. *See also* Gatewood, *supra* note 37, at 333 ("[T]he Supreme Court recognized trespass as the driving force for Fourth Amendment protection.").

45. *See* Gatewood, *supra* note 37, at 333–42 (discussing the Supreme Court's use of the "trespass doctrine" from *Olmstead* to *Katz* and how, even after *Katz*, *physical intrusion* into a constitutionally protected area was still the barometer in determining Fourth Amendment violations).

46. *See Jones*, 132 S. Ct. at 949. Justice Scalia, writing for the majority, stated:

> It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.

Id. (citing Entick v. Carrington, 95 Eng. Rep. 807 (C.P. 1765)).

Justice Scalia quotes the following passage in support of his view:

> [O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does his is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law. *Entick*, 95 Eng. Rep at 817.

47. *See, e.g.*, *Jones*, 132 S. Ct. at 949. *See also* Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that there was no violation of the defendant's Fourth Amendment rights because there was no trespassing into the home or

limitation on the government, but it also imposed a physical limitation.[48]

Even as trespass was (and is)[49] the ultimate barrier to intrusions into one's private life, other practical limitations, such as manpower, time, and other resources, played a significant role in preventing the government from delving too deeply into an individual's personal life prior to the technological advances of the twentieth century.[50] Prior to the advent of sophisticated surveillance tools, in order to amass the amount and detail of information that today's technology can do with relative ease, law enforcement would have been required to spend countless hours of manpower and financial resources to garner merely a fraction of the information.[51] Take for instance a hypothetical presented by former Chief Justice William H. Rehnquist in an article in 1974, just after he was appointed as Associate Justice to the Supreme Court.[52] In his hypothetical, Chief Justice Rehnquist asks whether the government should keep a "dossier of information pertaining to every citizen"[53] and offers the following hypothetical:

> Suppose that the local police in a particular jurisdiction were to decide to station a police car at the entrance to the parking lot of a well-patronized bar from 5:30 p.m. to 7:30 p.m. every business day for the purpose of making a list of the license plates of cars that were driven in and parked in the lot during that time. Presumably by appropriate checking with the motor vehicle division, the names of the registered owners of the cars could be obtained, and if there be at least a rebuttable likelihood that a car is generally driven by its registered owner, a reasonably accurate list of people who patronize the bar during these hours could be compiled.[54]

In posing this hypothetical, Chief Justice Rehnquist suggests that not only would a great majority of people find this kind of police activity an improper police function in terms of expenditure of taxpayer dollars[55] (and perhaps manpower),[56] but that, even if there was suffi-

---

curtilage of the defendant); Goldman v. United States, 316 U.S. 129, 135–36 (1942) (holding that the use of a electronic recording device did not violate the defendant's Fourth Amendment rights because there was no physical trespass into the home or curtilage of the defendant).

48. *See supra* notes 45–46 and accompanying text.
49. *See Jones*, 132 S. Ct. at 949. In relying on the trespass doctrine, the majority reasoned that applying common-law trespass principles best preserved the degree of privacy against government intrusion that existed at the time of the Fourth Amendment's adoption, stating that "[w]e have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id.*
50. *See supra* note 26 and accompanying text.
51. *See supra* note 27 and accompanying text.
52. *See* William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come a Long Way Baby*, 23 U. KAN. L. REV. 1 (1974).
53. *Id.* at 9.
54. *Id.*
55. *Id.*

cient manpower available to do it (which, in the context of a criminal investigation, he recognized to be a physically challenging task, particularly when more than one individual was implicated),[57] most people would disprove of such unwarranted surveillance.[58] While Chief Justice Rehnquist found his hypothetical facts too "extreme"[59] in 1974, they are not so "extreme" in the twenty-first century. Looking at today's license-plate scanners,[60] Chief Justice Rehnquist's then-hypothetical, is not so hypothetical anymore.[61] License-plate scanners can accomplish exactly what Chief Justice Rehnquist hypothesized in 1974 in a much more efficient manner today.[62] It has been estimated that automatic license-plate scanners are capable of scanning more than 1500 license plates per minute.[63] With this kind of efficiency, and undoubtedly cost-effectiveness, it is clear to see why law enforcement is steadfastly moving toward the use of such technology.[64]

License-plate scanners are just one example of how the use of technology has eroded many practical limitations, including those inferred by Justice Rehnquist's hypothetical. As new technologies in policing continue to emerge to address an ever-advancing society, any traditional practical limitation on Fourth Amendment invasions of privacy that once existed will continue to evaporate, putting pressure on Fourth Amendment freedoms.[65]

---

56. *Id.* (suggesting that some people may remark in response to his hypothetical that "if these police officers have nothing better to do, there ought to be a reduction in the staffing of the police department").
57. *Id.* at 10.
58. *Id.*
59. *Id.* Finding no privacy issue with his hypothetical, Justice Rehnquist nonetheless feels that "this ought not to be a governmental function when facts are as *extreme* as I put them." *Id.* (emphasis added).
60. According to some estimates, automatic license-plate recognition systems are capable of scanning more than 1500 license plates per minute. *See* Hilary Hylton, *License-Plate Scanners: Fighting Crime or Invading Privacy?*, TIME (July 30, 2009), http://www.time.com/time/nation/article/0,8599,1913258,00.html.
61. According to a recent survey conducted by the Police Executive Research Forum, 71% of responding agencies indicated they were using license-plate scanners. The survey also found that almost every police agency expects to acquire or increase their use of license-plate scanners and that within five years they expect that 25% of their vehicles will be equipped with license-plate scanners. *See Critical Issues in Policing Series, "How Are Innovations in Technology Transforming Policing?"*, POLICE EXECUTIVE RESEARCH FORUM, at iii (Jan. 2012) [hereinafter *Issues*], *available at* http://www.policeforum.org/critical-issues-series/ (follow "How Are Innovations in Technology Transforming Policing? (January 2012)" hyperlink).
62. *See* Hylton, *supra* note 60 and accompany text.
63. *Id.*
64. *See supra* note 61, at 1–4.
65. *See* Maclin, *supra* note 39, at 52 ("During the first-half of the twentieth century, Fourth Amendment liberties typically fared poorly under the pressure of a technologically advancing society.").

In addition to the erosion of practical considerations, the use of advance technology has necessitated a rigid interpretation of the Fourth Amendment—what a person knowingly exposes to the public, such as one's day-to-day movements along public streets, is not protected by the Fourth Amendment,[66] but once the government invades a constitutionally protected area ("persons, houses, papers, and effects")[67] without a warrant, the Fourth Amendment will be violated.[68] A brief look at the "search and seizure" issues confronted by the Supreme Court beginning in the twentieth century in response to new technology provides additional illustration of how the Supreme Court adapted the Fourth Amendment to address privacy concerns in the wake of ever-eroding practical limitations and fashioned a somewhat narrow and inflexible view of privacy in light of public and private expectations.

B. The Fourth Amendment and the Pressures Exerted by Advanced Technology

The technological advances in the last century or more have made it possible for law enforcement to achieve greater efficiency and become more effective at preventing and solving crime.[69] The effect of new technology has not only helped officers become more effective and efficient, but has made it possible to achieve this efficacy without invading, physically or in any other "private" sense recognized by the Supreme Court, the right of citizens "to be let alone."[70] This increased law enforcement efficacy has created pressure on Fourth Amendment privacy rights and polluted the scope of public and private expectations. A few examples of emerging technology used by law enforcement in the last century or more illustrate this point.

1. Wiretapping

One of the earliest uses of new technology by law enforcement was law enforcement's use of wiretapping.[71] Wiretapping began as soon as

66. Katz v. United States, 389 U.S. 347, 351 (1967).
67. U.S. CONST. amend. IV.
68. *See* U.S. v. Karo, 468 U.S. 705, 714 (1984); *see also* Kyllo v. U.S., 533 U.S. 27 (2001) (finding that if the "Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant").
69. *See Issues, supra* note 61, at iii.
70. Olmstead v. United States, 277 U.S. 438, 471 (1928) (Brandeis, J., dissenting) ("The makers of our Constitution . . . conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.").
71. *See* Howard, J. Kaplan et al, "*The History and Law of Wiretapping*," presented at ABA Section of Litigation 2012 Section Annual Conference April 18–20, 2012:

telephones were introduced in the 1870s.[72] While some states enacted piecemeal legislation to prohibit the use of wiretaps,[73] the use of wiretaps by law enforcement went relatively unchallenged until the 1920s when defendant Roy Olmstead challenged the use of wiretaps by federal law enforcement officers that resulted in his arrest and conviction.[74] In *Olmstead v. United States*,[75] federal agents installed wiretaps in the street near Olmstead's house and recorded conversations that were later used as evidence to convict Olmstead of conspiracy to violate the National Prohibition Act.[76] The Supreme Court held that wiretapping involves neither a search nor seizure within the meaning of the Fourth Amendment.[77] The Court reasoned that because there was no trespassing into Olmstead's home or the curtilage of his home, there was no "search" within the meaning of the Fourth Amendment.[78] Thus, the "trespass doctrine"[79] was born. *Olmstead* represents a sharp demarcation by the Supreme Court between that which is public (streets outside the home)[80] and that which is private

---

The Lessons of the Raj Rajaratnam Trial: Be Careful Who's Listening, at 2 ("Wiretapping has existed for as long as oral communications have been transmitted over wires. After the invention of the telegraph in 1837 and the telephone in 1876, private detectives tapped wires for their clients, and businesses tapped each other's wires in a nineteenth-century version of corporate espionage."), *available at* http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/29-1_history_and_law_of_wiretapping.authcheckdam.pdf.

72. *Id.*

73. *Id.*

74. *See generally* United States v. Olmstead, 277 U.S. 438 (1928).

75. *Id.*

76. *Id.*

77. *Id.* at 464 (holding that the Fourth Amendment did not prohibit wiretapping in that "[t]here was no searching. There was no seizure. The evidence was secured by use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.").

78. *Id.* at 466. The Court explained that "one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them, are not within the protection of the [Fourth] Amendment." *Id.*

79. The "trespass doctrine" in Fourth Amendment jurisprudence is based on the concept that "the [F]ourth [A]mendment protected 'persons, houses, papers, and effects' when these entities were located within a 'constitutionally protected area.'" David P. Miraldi, Comment, *The Relationship Between Trespass and Fourth Amendment Protection After* Katz v. United States, 38 OHIO ST. L.J. 709, 710 (1977); *see also Goldman*, 316 U.S. 129, 134–35 (relying on the opinion in *Olmstead*, the Supreme Court held that the use of an electronic recording device did not violate the defendant's Fourth Amendment rights because there was no physical trespass into the defendant's home or curtilage).

80. *See Olmstead*, 277 U.S. at 465 ("The language of the [Fourth Amendment] cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office.").

(inside the home).[81] Thus, property lines marked the degree of privacy one was afforded.

Even with this strong demarcation, tension was evident in *Olmstead* that there was a need for the Fourth Amendment to adapt to technological advances. Justice Brandeis's dissenting opinion in *Olmstead* illustrates the tension between the traditional guarantees of the Fourth Amendment against specific governmental abuses of power and the need to adapt for an ever-changing world. Justice Brandeis writes:

> When the Fourth and Fifth Amendments were adopted, "the form that evil had heretofore taken" had been necessarily simple. Force and violence were then the only means known to man by which a government could directly effect self-incrimination. It could compel the individual to testify—a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life—a seizure effected, if need be, by breaking and entry. Protection against such invasion of "the sanctities of a man's home and the privacies of life" was provided in the Fourth and Fifth Amendments by specific language. But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.[82]

Justice Brandeis was addressing not only the right of individuals, but also of criminals, to be free from having conversations intended to be private intercepted by the government, notwithstanding the lack of a physical trespass or other intrusion onto the person or property.[83]

In the area of wiretapping, this tension persisted for many years. Although Congress outlawed wiretapping in 1934 when it passed the Communications Act of 1934,[84] which became applicable to private citizens in 1937,[85] it was not until 1967 that the Supreme Court in *Katz v. United States*[86] ruled that wiretapping was a "search" within the meaning of the Fourth Amendment.[87] In *Katz*, FBI agents recorded the defendant's conversations using an electronic listening and recording device attached to the exterior of a telephone booth.[88] The Court concluded that the government's "activities in electronically lis-

81. *Id.* at 466 (finding that a person's Fourth Amendment rights have not been violated "unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage . . . .'").
82. *Id.* at 473 (citations omitted).
83. *See id.* at 457.
84. Communications Act of 1934, ch. 652, 48 Stat. 1064 (1934) (current version at 47 U.S.C. §§ 151–620 (2012)).
85. *See* Nardone v. United States, 302 U.S. 379 (1937).
86. 389 U.S. 347 (1967).
87. *Id.*
88. *Id.* at 348.

tening to and recording the [defendant's] words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[89] In addressing this issue, the tension between the rigidity of the Fourth Amendment (i.e., "Whether physical penetration of a constitutionally protected area is necessary before a search and seizure can be said to be violative of the Fourth Amendment to the United States Constitution")[90] and need to adapt the Fourth Amendment to address emerging technology is clearly evident in the Court's holding in the following excerpt:

> We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.[91]

Katz marked a new direction in Fourth Amendment jurisprudence with regard to electronic surveillance while adopting a newly formulated test for determining when a "search" had occurred,[92] which became known as the reasonable expectation of privacy test.[93] The *Katz* reasonable expectation of privacy test informed the Supreme Court's decision in many later uses of new technologies. This newly formulated test, however, seemed to create a new rigid approach to Fourth Amendment violations—that between public and private expectations.

2. Pen Registers

Pen registers allow law enforcement officials to record the phone numbers of all outgoing calls from a particular phone. This technology was used by law enforcement officials in *Smith v. Maryland*.[94] In *Smith*, at the request of law enforcement, the telephone company installed a pen register at its offices to record the numbers dialed from

89. *Id.* at 353.
90. *Id.* at 350.
91. *Id.* at 353.
92. Under Justice Harlan's concurring opinion, the Court adopted a two-pronged test for determining when a "search" had occurred. The first prong considers whether the defendant had an actual or subjective expectation of privacy that was violated, and the second prong considers whether that "expectation [is] one that society is prepared to recognize as 'reasonable.'" *Id.* at 361 (Harlan, J., concurring) (citations omitted).
93. *Id.*
94. 442 U.S. 735 (1979).

the petitioner's telephone.[95] In the majority's opinion, Justice Blackmun rejected the notion that the installation and use of a pen registry violated a "legitimate expectation of privacy"[96] of the defendant since the pen register was installed on telephone company property at the telephone company's central offices.[97] The Court explained that the defendant had no actual expectation of privacy because "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed [and that] [a]ll subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills."[98] The Court further explained that even if the defendant had a subjective expectation of privacy, this expectation is not "one that society is prepared to recognize as 'reasonable'"[99] because the numbers dialed were made *public* to the phone company.[100]

Compelling the Court's reasoning, which the Court expressly clarified,[101] was the fact that "the pen register was installed on telephone company property at the telephone company's central offices,"[102] and, therefore, the defendant clearly could not claim that his property was invaded or that a "constitutionally protected area" was invaded by the police. The Court's need to clarify the exact nature of the conduct challenged by the defendant was dispositive of the Court's awareness of the tension between private and public expectations and further illustrates the Court's rigid Fourth Amendment formulation regarding public and private expectations—what is publically disseminated loses its Fourth Amendment protection.[103]

---

95. *Id.* at 737.

96. *Id.* at 742.

97. *Id.*

98. *Id.*

99. *Id.* at 743 (citations omitted).

100. *Id.* at 743–44.

101. *Id.* at 741 ("In applying the *Katz* analysis to this case, it is important to begin by specifying precisely the nature of the state activity that is challenged. The activity here took the form of installing and using a pen register. Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner obviously cannot claim that his 'property' was invaded or that police intruded into a 'constitutionally protected area.' Petitioner's claim, rather, is that, notwithstanding the absence of a trespass, the State, as did the Government in *Katz*, infringed a 'legitimate expectation of privacy' that petitioner held.").

102. *Id*.

103. *Id.* at 743–44.

3. Beepers

The Supreme Court first considered the use of beeper technology in *United States v. Knotts*.[104] While the Court ultimately found that the warrantless use of a beeper tracking device to track a suspect's movements along public streets did not violate the Fourth Amendment,[105] the Court left open the possibility that the use of enhanced surveillance technology, even if done in public, may not always pass constitutional scrutiny.[106] This question left open by the Court highlights the Court's unwillingness, despite technological advances, to deviate from its rigid interpretation of the Fourth Amendment that one has no reasonable expectation of privacy while in public.[107]

In *Knotts*, Minnesota law enforcement arranged to have a beeper placed inside a container of chloroform purchased by the defendant and used the beeper's signal to track the suspect back to his cabin, where they found an illegal drug operation.[108] The Court concluded that although the defendant may have had a subjective expectation of privacy in his movements, "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[109] The Court found no relative difference between the surveillance technology used and the surveillance itself because following the beeper's signal was analogous to visually following the vehicle on the public streets and highways[110] and because there was no indication that the beeper was used to re-

104. 460 U.S. 276 (1983).

105. *Id.* at 285 (employing the *Katz* reasonable expectation of privacy test, the Court held that monitoring beeper signals was "neither a 'search' nor a 'seizure' within the contemplation of the Fourth Amendment" because monitoring beeper signals did not invade any reasonable expectation of privacy of the suspect).

106. In response to the Government's contention that the Court's ruling may lead to "twenty-four hour surveillance of any citizen," the Court stated, "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Id.* at 283–84 (citation omitted).

107. *See id.* at 281; *see also* Florida v. Riley, 488 U.S. 445, 450–51 (1989) (holding aerial observation of the defendant's home during helicopter flyover was not a search under Fourth Amendment); California v. Greenwood, 486 U.S. 35, 41–42 (1988) (holding no reasonable expectation of privacy in trash left at curbside outside defendant's home); Dow Chem. Co. v. United States, 476 U.S. 227, 237–39 (1986) (holding aerial observation of an industrial plant was not a search under Fourth Amendment); California v. Ciraolo, 476 U.S. 207, 213 (1986) (holding aerial observation of curtilage of defendant's home was not a search).

108. *Knotts*, 460 U.S. at 277–79.

109. *Id.* at 281.

110. *See id.* at 285. Furthermore, the Court noted "[t]he fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper to signal . . . does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case." *Id.* at 281.

veal any information inside the defendant's home.[111] Therefore, because all of the defendant's movements could be observed publicly there was no constitutional objection. However, when the same issue came before the Supreme Court in *United States v. Karo*,[112] just over a year later, the Court held that monitoring of a beeper signal while located in a *private* residence closed to visual surveillance was a violation of the Fourth Amendment and the rights of "those who ha[d] a justifiable interest in the privacy of the residence."[113]

Knotts and *Karo* strongly reflect the dichotomy in the Supreme Court's approach to new technology and the Fourth Amendment, which ultimately preserves the division between the public and private realms.

4. Thermal Imaging

Thermal imaging illustrates a more novel example of how the Supreme Court has preserved the dichotomy between public and private expectations in the wake of new technology. The Supreme Court considered thermal imaging in *Kyllo v. United States*.[114]

In *Kyllo*, police directed a thermal imaging device at the home of the defendant, who was suspected of growing marijuana, to determine if the amount of heat coming from his home was consistent with the heat that emanates from high-intensity lamps typically used to grow marijuana.[115] The Court held that use of thermal imaging technology constituted a search under the Fourth Amendment because the use of the technology allowed the government to obtain information about the inside of the home that was not otherwise accessible without a physical intrusion.[116] In essence, the Court's ruling limited Fourth Amendment invasions of privacy to those originally thought to be protected when the Fourth Amendment was adopted.[117] However, even though the Court seemed concerned that the use of police technology may erode such Fourth Amendment guarantees,[118] the Court may

111. *Id.* at 285.
112. 468 U.S. 705, 708–10. In *Karo*, DEA agents used a beeper contained in a can of ether purchased by the defendant to track his movements, which eventually led the agents to a residence rented by the defendant, where they found illegal drug manufacturing equipment.
113. *Id.* at 714.
114. 533 U.S. 27 (2001).
115. *Id.* at 30.
116. *Id.* at 40.
117. *Id.* at 34 (explaining that its holding "assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted").
118. *Id.* at 34 (acknowledging that the home was the prototypical area of protected privacy, the Court stated, "[t]o withdraw protection of [privacy of the home] would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment").

have essentially unwittingly gutted those Fourth Amendment protections by intimating that if the technology used was in general public use, even the home may not be protected against technological innovations.[119]

Nevertheless, it was apparent from the Court's holding that technology can push the Fourth Amendment boundary between that which is public and that which is private to its furthest limits[120] and blur the scope of Fourth Amendment protections.[121]

Kyllo's return to historical Fourth Amendment guarantees was echoed in the recent Supreme Court decision regarding GPS technology.

5. GPS Devices

The Supreme Court again returned to the traditional notions of Fourth Amendment guarantees in *United States v. Jones*.[122] The Court, ignoring all recent precedent, held that the warrantless installation and subsequent use of a GPS tracking device to track the movement of a suspect's vehicle violated the Fourth Amendment.[123] Justice Scalia, writing for the majority, focused exclusively on common law trespass to resolve the issue.[124] While the *Jones* opinion was unanimous, the Justices were split five to four on which constitutional precedent to use to resolve the issue—the K*atz* reasonable expectation of privacy test or the trespass doctrine.

In relying on the trespass doctrine, the majority rationalized that applying common law trespass principles best preserves the degree of privacy afforded by the Fourth Amendment at the time of its adoption.[125] The concurring opinions of Justices Sotomayor and Alito criti-

119. *Id.* at 34 ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use.") (citations omitted).

120. *Id.* at 33–34 ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

121. *Id.* at 31 ("The permissibility of ordinary visual surveillance of a home used to be clear because, well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass.").

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

123. *Id.* at 948–54.

124. *Id.* at 949–50.

125. *Id.* at 949 ("We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

cized the majority use of the trespass doctrine and raised several questions left unanswered by Justice Scalia's approach.[126]

Justice Sotomayor thought that the issue should have been resolved by focusing on social norms and societal expectations.[127] She wrote, "I would take [the] attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements."[128] She stated more specifically that "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[129] Justice Alito would have focused on the *Katz* reasonable expectation of privacy test to resolve the issue, although he noted that the *Katz* test was not without its own problems.[130]

The varying opinions of the Justices in *Jones* make it patently clear that new technology poses a risk to Fourth Amendment privacy rights that are so complex and varying that the Justices have chosen to punt on most of the critical issues, leaving them to be addressed, perhaps, another day.[131] Not only have the Justices decided to reserve critical issues for later discussion or legislative enactment,[132] but they have continued down a path that almost ensures that use of new technology, particularly surveillance and tracking technology, continues to erode away at traditional practical limitations that once defined Fourth Amendment protections, while redefining the scope of privacy in a way that ensures all our public movements are susceptible to scrutiny by law enforcement at anytime and anywhere.

So, what is the correct resolution? One might find the answer in a theory originating from a series of cases involving challenges by the government to requests under the Freedom of Information Act (FOIA)—the mosaic theory,[133] which was adapted for Fourth Amendment use in *Maynard*.[134] Curiously enough, a majority of the Su-

126. *See id.* at 954–57 (Sotomayor, J., concurring), 957–64 (Alito, J., concurring in judgment).

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

128. *Id.*

129. *Id.*

130. *See id.* at 958, 962 (Alito, J., concurring in judgment) (finding the *Katz* test preferable but noting difficulties inherent in the test).

131. *Id.* at 954 (majority opinion) ("We may have to grapple with these 'vexing problems' in some future case . . . .").

132. *Id.* at 962 (Alito, J., concurring in judgment) ("[C]oncern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions.").

133. *See generally* Pozen, *supra* note 11.

134. *See* United States v. Maynard, 615 F.3d 544, 560–63 (D.C. Cir. 2010), *aff'd sub nom*. United States v. Jones, 132 S. Ct. 945 (2012).

preme Court appears willing to accept this new theory of Fourth Amendment jurisprudence.[135]

III. THE MOSAIC THEORY AND THE FOURTH AMENDMENT

A. The Origins of the Mosaic Theory

The mosaic theory finds its genesis in cases involving national security where the government sought to block information requests under the Freedom of Information Act (FOIA).[136] The mosaic theory describes how "apparently harmless pieces of information when assembled together could reveal a damaging picture."[137] The government has successfully invoked the mosaic theory on numerous occasions to justify withholding documents requested under FOIA.[138] The theory was first articulated in *United States v. Marchetti*.[139]

In *Marchetti*, the government sought to enjoin a former CIA employee from publishing a book, which, according to the government, contained classified information concerning intelligence sources, methods, and operations.[140] Although the Court granted the government's injunction, it did so based upon the executive right to secrecy under the Constitution and the secrecy agreement signed by the for-

135. *See supra* note 21 and accompanying text.

136. *See generally* Pozen, *supra* note 11. Pozen's Note provides an informative summary of the development and use of the mosaic theory since its first use in 1972 to defeat requests made under the Freedom of Information Act (FOIA) in the name of national security. FOIA is a federal statute granting a right of public access to certain governmental information. *See* 5 U.S.C. § 552 (2012).

137. 32 C.F.R. § 701.31 (2010). *See also* Pozen, *supra* note 11, at 630 ("The 'mosaic theory' describes a basic precept of intelligence gathering: Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information. Combining the items illuminates their interrelationships and breeds analytic synergies, so that the resulting mosaic of information is worth more than the sum of its parts. In the context of national security, the mosaic theory suggests the potential for an adversary to deduce from independently innocuous facts a strategic vulnerability, exploitable for malevolent ends.").

138. *See, e.g.*, CIA v. Sims, 471 U.S. 159, 168–74 (1985) (holding that the CIA was not required to disclose the institutional affiliates of CIA-funded researchers who were previously found to be "intelligence sources"); Ctr. for Nat'l Sec. Studies v. U.S. Dep't. of Justice, 331 F.3d 918, 935–36 (D.C. Cir. 2003) (holding that the Department of Justice was not required to disclose information regarding detained individuals after a significant terrorist attack); New Jersey Media Grp., Inc. v. Ashcroft, 308 F.3d 198, 218–21 (3d Cir. 2002) (denying access to the media on the basis of national security to certain deportation hearings); Hunt v. CIA, 981 F.2d 1116, 1119–21 (9th Cir. 1992) (denying request for CIA records of an Iranian national); Halkin v. Helms, 598 F.2d 1, 8–10 (D.C. Cir. 1978) (using "mosaic theory" to support finding of state secrets privilege). *See also* Pozen, *supra* note 11, at 630–31 (discussing historical use of FOIA).

139. 466 F.2d 1309, 1318 (4th Cir. 1972).

140. *Id.* at 1311–13.

mer employee.[141] But in so doing, the Court gave a sweeping justification:

> The 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. The courts, of course, are ill-equipped to become sufficiently steeped in foreign intelligence matters to serve effectively in the review of secrecy classifications in that area.[142]

After *Marchetti*, the mosaic theory was used cautiously,[143] but it gained prominence after the 9/11 terrorist attacks on the World Trade Center.[144] Today, the mosaic theory in national security is gaining an ever-expanding role in the age of information technology and nonconventional terrorism,[145] and mosaic claims have proven to be unimpeachable.[146]

B. *Maynard*, *Jones*, and the Mosaic Theory

1. The Maynard *Decision*

A mosaic theory argument was first expounded in the context of the Fourth Amendment in *United States v. Maynard*.[147] In *Maynard*, co-conspirators Lawrence Maynard and Antoine Jones appealed their 2008 convictions for conspiracy to distribute and possession with intent to distribute cocaine and cocaine base.[148] The appeal addressed several issues, none of which warranted reversal,[149] except the issue of whether defendant Jones's Fourth Amendment rights were violated when law enforcement installed a GPS tracking device on Jones's vehicle without a warrant and tracked his movements for four weeks, twenty-four hours a day.[150] While several district courts addressing this issue at the time concluded that such monitoring did not constitute a "search" under the Fourth Amendment,[151] relying exclusively

141. *See id.* at 1315–18.
142. *Id.* at 1318.
143. *See* Pozen, *supra* note 11, at 638–41.
144. *See id.* at 630–31.
145. *Id.* at 678–79.
146. *Id.* at 679 ("In over thirty years of the theory's existence, only one FOIA court on record has rejected a government agency's mosaic defense.").
147. *See* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).
148. *Id.* at 549.
149. *Id.*
150. *Id.* at 555.
151. *See* United States v. Cuevas-Perez, 640 F.3d 272 (7th Cir. 2011); United States v. Marquez, 605 F.3d 604, 609–10 (8th Cir. 2010) (noting that even if the defendant had standing to raise the Fourth Amendment issue, his argument would fail because the GPS unit was not a "search"); United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010); United States v. Garcia, 474 F.3d 994 (7th Cir. 2007).

on principles articulated in *Knotts* that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,"[152] the *Maynard* court came to a different result.

Judge Douglas Ginsburg, writing for the majority, broke the issue down into separate discrete questions that he addressed in order. Judge Ginsburg first examined whether *Knotts* was controlling.[153] In addressing this question, the court reasoned that *Knotts* was not controlling since *Knotts* dealt with limited information discovered by use of a beeper during a single discrete trip[154] and did not deal with the type of "prolonged twenty-four hour surveillance"[155] explicitly reserved by *Knotts*.[156] Judge Ginsberg noted that *Knotts* did not hold that "a person has no reasonable expectation of privacy in his movements whatsoever, world without end . . . ."[157]

Having concluded that *Knotts* was inapplicable, Judge Ginsburg turned to the second question of whether the defendant had a reasonable expectation of privacy in his public movements that society was prepared to recognize as reasonable.[158] For Judge Ginsburg, the answer to this question depended, in large part, on whether the reasonable expectation of privacy related to information that had been "expose[d] to the public."[159] This analysis required Judge Ginsburg to consider whether Jones's movements had been actually or constructively exposed to the public.[160]

On the question of actual exposure, the court found that the defendant's movements had not actually been exposed to the public because of the slim likelihood that anybody would observe all of his movements over a month.[161] The focus was not what another was physically or

152. United States v. Knotts, 460 U.S. 276, 281 (1983).

153. *Maynard*, 615 F.3d at 556–58.

154. *Id.* at 556.

155. *Id.* at 557.

156. *Id.* at 556–57. *See also Knotts*, 460 U.S. at 284 (dispensing with defendant's argument that without judicial oversight of the use of enhanced surveillance, any citizen could be the target of constant twenty-four hour surveillance, by noting, "if such dragnet-type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.").

157. *Maynard*, 615 F.3d at 557.

158. *Id.* at 558.

159. *Id.* at 558 (alteration in original) (citing United States v. Katz, 389 U.S. 347, 351 (1967)).

160. *Id.* at 558–59.

161. *Id.* at 558 ("[T]he totality of Jones's movements over the course of a month was . . . not exposed to the public: First, unlike one's movements during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil.").

lawfully able to do but what a "reasonable person expects another might actually do."[162] Judge Ginsburg notes:

> It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.[163]

To address the question of constructive exposure—whether each of the defendant's individual movements during the four-week prolonged surveillance was itself in public view[164]—Judge Ginsburg turned to *United States Department of Justice v. Reporters Committee of the Freedom Press*,[165] which arose under the FOIA. In that case, the FBI refused to disclose "rap sheets" of certain individuals even though the raps sheets were compiled with individual events that were already a matter of public record.[166] The Supreme Court reasoned, "[T]here is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[167] The *Maynard* court agreed and applied a similar reasoning:

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[168]

Judge Ginsburg additionally noted that while discrete pockets of movements of the defendant may have been exposed to the public:

> The whole of one's movements over the course of a month is not constructively exposed to the public, because like a rap sheet, that whole reveals far more than the individual movements it comprises. The difference is not one of de-

162. *Id.* at 559.
163. *Id.* at 560.
164. *See id.* at 560–61.
165. 489 U.S. 749 (1989).
166. *Id.* at 757.
167. *Id.* at 764.
168. *Maynard*, 615 F.3d at 562.

> gree but 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.[169]

In the re-styled case, *United States v. Jones*,[170] the Supreme Court reviewed *Maynard* and affirmed the D.C Circuit's ruling, but on entirely different reasoning.

2. The Jones *Decision*

As discussed above,[171] the Supreme Court unanimously agreed with the D.C. Circuit in *Maynard* that Jones's Fourth Amendment rights were violated when the government installed and subsequently used a GPS tracking device to track Jones's movements along public roads for four weeks, twenty-four hours a day.[172] In resolving the issue, the Supreme Court opted to return to the origins of the Fourth Amendment, adopting common-law trespass as the rationale for its decision.[173] While the majority's opinion never broached the mosaic theory, Justice Alito's concurring opinion, joined by Justices Ginsburg, Breyer, and Kagan, as well as Justice Sotomayor's concurring opinion, each seemed to embrace the rationale of the mosaic theory, at least in principle.[174]

Justice Alito's concurrence focused on "whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove."[175] He conceded that *Knotts* was only applicable to "relatively short-term monitoring of a person's movements."[176] But he echoed the D.C. Circuit's mosaic theory in *Maynard*, stating that "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue *every single movement* of an individual's car for a very long period."[177]

Justice Sotomayor's concurrence likewise endorsed a mosaic approach. The unique attributes of GPS monitoring, led her to ask "whether people reasonably expect that their movements will be recorded and *aggregated* in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sex-

169. *Id.* at 561–62.

170. United States v. Jones, 132 S. Ct. 954 (2012).

171. *See supra* subsection II.B.5.

172. *Jones*, 132 S. Ct. at 948–54.

173. *Id.* at 949–50.

174. *See id.* at 964 (Alito, J., concurring); *Jones*, 132 S. Ct. at 955–56 (Sotomayor, J., concurring); *supra* note 21 and accompanying text.

175. *Jones*, 132 S. Ct. at 958 (Alito, J., concurring in judgment).

176. *Id.* at 964.

177. *Id.* at 964 (emphasis added).

ual habits, and so on."[178] Her focus was on whether there are Fourth Amendment rights "in the sum of one's public movements."[179]

Both Justice Alito's and Justice Sotomayor's separate concurring opinions clearly indicate resound approval of the principles of the mosaic theory and reflect a five-Justice majority of the Supreme Court.

C. Issues Regarding the Implementation of the Mosaic Theory

The introduction of the mosaic theory into Fourth Amendment jurisprudence has met with mixed reaction.[180] Those that support the newly formulated theory are staunch supporters,[181] while those that oppose the new theory are adamant in their opposition.[182] Whatever side one happens to fall on, the criticism of the mosaic theory is generally the same.[183]

The first issue raised by the adoption of the mosaic theory into Fourth Amendment jurisprudence is how to determine the scope of the mosaic necessary to create a Fourth Amendment violation.[184] In other words, how much is too much? The *Maynard* decision did not express a bright-line rule regarding how much surveillance is required to create a mosaic sufficient to violate the Fourth Amendment.[185] In addition, it has been proffered that the pro-mosaic opinions authored in *Maynard* (Judge Ginsburg) and *Jones* (Justices Alito and

178. *Id.* at 956 (Sotomayor, J., concurring) (emphasis added).

179. *Id. See also* Kerr, *supra* note 21, at 328 ("Justice Sotomayor focuses on whether a person has Fourth Amendment rights 'in the sum' of their public movements, rather than in individual movements").

180. *See supra* note 22 and accompanying text.

181. *See supra* note 23 and accompanying text.

182. *Id.*

183. *See* Dennis, *supra* note 22; Dickman, *supra* note 22; Ford, *supra* note 22.

184. *See* Kerr, *supra* note 21, at 330 ("The first challenge raised by the potential adoption of a mosaic theory is selecting the proper standard for aggregation. This question divides into two parts. The first requires identifying the proper reference point for when a mosaic has been created. The second requires choosing which stages of surveillance that the mosaic theory regulates . . . ."). *See also* Ostrander, *supra* note 22, at 1749 ("[W]ho has the burden of proof with respect to whether the prolonged surveillance has in fact revealed an intimate picture of an individual's life and thus created a mosaic?").

185. *See Maynard*, 615 F. 3d at 558, 560. *See also* Ostrander, *supra* note 22, at 1748 ("*Maynard* left little guidance as to what durational threshold must be crossed in order for the use of pattern-detecting technology to be sufficiently prolonged as to render it a search. Without a clearly demarcated line, law enforcement agents, judges, and individuals cannot know when an aggregate of information will receive Fourth Amendment protection.") (footnote omitted).

Sotomayor) each suggest a different answer.[186] This ambiguity makes it difficult to apply the mosaic theory.[187]

The second major criticism, and perhaps just as problematic as the first, is determining what search methods trigger the mosaic theory.[188] What if the government used cell phone location data, pen registry data, wiretaps, GPS surveillance, and visual surveillance?[189] Which, if any of these modes of surveillance, would be acceptable for the purpose of a mosaic? What if one mode of surveillance only reveals limited information? Does that mode of surveillance get aggregated with all other modes of surveillance or just with similar or the same modes?[190] According to opponents of the mosaic theory, these questions would need to be addressed if the mosaic theory were adopted.[191]

Perhaps the most critical issue raised with respect to adoption of the mosaic theory is the retroactive unconstitutionality that the mosaic theory may create.[192] It is conceivable that individual components of a search would not, in and of themselves, constitute a search under any theory of the Fourth Amendment. But when all the pieces are aggregated together, the mosaic may reveal far more than the individual pieces, making the individual pieces retroactively unconstitutional.[193]

The above, while not exhaustive, could have a chilling effect on law enforcement's exercise of the full extent of their investigatory power if the mosaic theory is adopted.[194] But that is exactly the point. Adop-

186. *See* Kerr, *supra* note 21, at 330 ("The three pro-mosaic opinions in *Maynard*/*Jones* each suggest a different answer. Justice Alito focused on societal expectations about law enforcement practices . . . . Justice Sotomayor offered a more normative standard that looked at government power . . . . Judge Ginsburg . . . [focused] on whether the government learned more than a stranger could have observed.") (footnotes omitted).

187. *See id.* at 330–31.

188. *Id.* at 334.

189. Some or all of these search modes were used to investigate the defendants in *Maynard*. *See Maynard*, 615 F.3d 544.

190. *See* Kerr, *supra* note 21, at 335 ("If the mosaic theory applies to multiple surveillance methods, courts must also consider whether the duration and scale questions raised earlier should be answered in the same way for every method. Different methods of surveillance have different levels of invasiveness. As a result, different methods of surveillance might require different regulation within the mosaic framework.").

191. *Id.*

192. *See* Ostrander, *supra* note 22, at 1748–49 ("As soon as a pattern is created, previously permissible individual law enforcement steps become unconstitutional.").

193. *See* Walsh, *supra* note 22, at 235.

194. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH L. REV. 801, 883–84 (2004) ("[I]nterstitial rulemaking that leaves the rules unclear lessens the clarity of the limits on the government's powers to invade privacy, underdeterring police behavior in some contexts and overdeterring it in others."); *id.* at 861 ("The rules of

tion of the mosaic theory will force law enforcement officials to adopt guidelines and procedures and make critical decisions regarding the use of certain investigatory techniques so as to avoid having valuable evidence excluded, erring on the side of caution by obtaining a warrant or utilizing their investigatory methods in a less intrusive or abusive manner. In the wake of advanced technology, the mosaic theory will provide a balancing effect—equilibrium if you will—between Fourth Amendment privacy rights and the need for effective and efficient law enforcement by restoring the practical considerations that once limited the extent to which law enforcement could intrude on one's privacy without violating the Fourth Amendment.

IV. EQUILIBRIUM EFFECT OF THE MOSAIC THEORY

A. The Mosaic Concept

Despite the varying and complex issues regarding the implementation of the mosaic theory, this Article proffers that the mosaic theory may be a viable solution for the protection of Fourth Amendment privacy rights in the wake of advanced surveillance and tracking technology. However, in order to truly appreciate the complexity of introducing the mosaic theory into Fourth Amendment jurisprudence, it is first necessary to understand what is at stake. Take, for instance, the bombings during the 2013 Boston Marathon.

On April 15, 2013, two pressure cooker bombs exploded during the Boston Marathon seconds apart, killing three people and injuring 265.[195] With the aid of surveillance cameras,[196] private security cameras, and photos shot by bystanders on smartphones, it took the FBI only three days to identify the two suspects.[197] Arguably, without the aid of surveillance cameras, the suspects may have continued their

---

criminal procedure . . . tell government agents what they can and cannot do to collect evidence of crime and identify wrongdoers. Because these rules limit government power, rule clarity minimizes official discretion and encourages compliance. Unclear rules mean unclear limits on government power, increasing the likelihood of abuses by aggressive government officials.") (footnotes omitted).

195. *See* Miranda Leitsinger, *Marathon Bomb Victims Adjust to a 'Different Normal*,' NBC NEWS, (May 15, 2013), http://usnews.nbcnews.com/_news/2013/05/15/18256453-marathon-bomb-victims-adjust-to-a-different-normal?lite.

196. According to estimates in 2007, there were 147 surveillance cameras operated by Boston city officials. *See* Henry Ridgwell, *Boston Bombing Sparks Surveillance Camera Debate*, VOICE OF AMERICA, (Apr. 24, 2013), http://www.voanews.com/content/boston-bombing-sparks-surveillance-camera-debate/1648071.html.

197. "Former FBI Special Agent Peter J. Ahearn says surveillance cameras are one of the primary tools of investigation. 'The first thing you do in any kind of a crisis in an area is you go for the tapes, you go for the video. The ATM machines, anything on the street and there will be a team of investigators and analysts working that.'" *Id.*

terrorist rampage.[198] Despite the numerous calls for privacy in the wake of increased use of surveillance cameras across the country,[199] few would argue against the use of surveillance cameras in Boston on that infamous April 15th day.[200] In fact, in the wake of the Boston bombings, there was increased interest in the use of surveillance cameras across the country.[201] So, how do we begin to balance the need for the type of surveillance used so successfully in Boston and the need for law enforcement to investigate and prevent crime with society's need to have some measure of privacy, especially in public? Specifically, how do we balance society's reasonable expectation of privacy in one's public movements with the practical guarantees of the Fourth Amendment, while allowing law enforcement officials the necessary latitude to investigate and prevent crime, especially under the current proscriptions of the Fourth Amendment? Of course, there are times when the collection, recording, and storage of information en mass is a good thing—case in point, Boston. But there are times when such collection, recording, and storage do not comport with the reasonable expectations of society's view of privacy. So what is the correct answer? Ultimately, the answer may lie with the application of the mosaic theory.

B. Application of the Mosaic Theory

There are two extreme competing interests in the debate concerning privacy and advance surveillance technologies: society's reasonable expectation of privacy in their public movements and law enforcements need to properly investigate and prevent crime. However, as aptly put by President Obama in a press conference on June 7, 2013, concerning revelations of massive data mining by the National

198. *See* Greg Botelho & Josh Levs, *Boston Bombing Suspects Planned Times Square Attack, Bloomberg Says*, CNN, (Apr. 25, 2013), http://www.cnn.com/2013/04/25/us/boston-attack.

199. *See, e.g.*, Geoffrey R. Stone, *The Boston Bombing, the Right of Privacy and Surveillance Cameras*, Post in *The Blog*, HUFFINGTON POST (May 6, 2013, 1:15 PM), http://www.huffingtonpost.com/geoffrey-r-stone/the-boston-bombing-the-ri_b_3223871.html ("The practice of using surveillance cameras to record our comings and goings is ever-expanding, and will certainly expand still further after the Boston bombings.").

200. *But see* Heather Kelly, *After Boston: The Pros and Cons of Surveillance Cameras*, CNN (April 26, 2013), http://www.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings. ("We like to think we have some privacy in our lives, that we can go places that we don't necessarily want the government to know about," said Jennifer Lynch, an attorney at the Electronic Frontier Foundation, an Internet civil-liberties group. "What concerns me is if all of those cameras get linked together at some point, and if we apply facial recognition on the back end, we'll be able to track people wherever they go.").

201. *See, e.g.*, *Boston Attacks Inspire Use of Surveillance Cameras in Cities Nationwide*, PBS (May 15, 2013), *available at* http://www.pbs.org/newshour/bb/nation/jan-june13/surveillance_05-15.html.

Security Agency,[202] "We're going to have to make some choices as a society. . . . It's important to recognize that you can't have 100 percent security and also then have 100 percent privacy and zero inconvenience."[203] This is where the mosaic theory comes into play.

Under the current proscriptions of the Fourth Amendment, in investigating crimes, law enforcement officials require a warrant supported by probable cause[204] or, in some cases, just probable cause or reasonable suspicion that a crime has been or will soon be committed.[205] In the latter instances, when law enforcement is operating without a warrant, the reasonableness of the government's conduct under the Fourth Amendment can be a difficult question to address in light of the varying constitutional thresholds that may be applicable to the government's conduct. For example, when the government searches a home, a warrant supported by probable cause is generally required.[206] However, when the government searches a motor vehicle, only probable cause is required, and no warrant is necessary.[207] Searches of individuals for weapons only require reasonable suspicion.[208] In the advent of advanced surveillance and tracking technology, the applicable constitutional reasonableness standards can become even more muddled because these technologies can be used without violating any constitutional reasonableness standard under the current proscriptions of the Fourth Amendment.[209] As such, traditional Fourth Amendment guarantees have waned in the face of advanced surveillance and tracking technology. On the other hand, the need for effective and diligent law enforcement efforts is ever more important in what may be becoming a terroristic technological society. The mosaic theory offers a way to restore the equilibrium between the traditional privacy protections that practical limitations safeguarded in the pre-computer age[210] and the need for vigilant law enforcement.

202. *See* Sam Stein, *NSA Surveillance Program Oversight: White House, Congress Point Fingers at Each Other*, HUFFINGTON POST (June 7, 2013), http://www.huffingtonpost.com/2013/06/07/nsa-surveillance-program-oversight_n_3405716.html.
203. *See* Lara Jakes & Darlene Superville, *Obama Defends NSA, Says America Has to Make Choices Between Privacy and Security*, HUFFINGTON POST (June 7, 2013), http://www.huffingtonpost.com/2013/06/07/obama-defends-nsa_n_3406448.html.
204. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").
205. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 30 (1968).
206. *See* United States v. Karo, 468 U.S. 705 (1984).
207. *See* California v. Carney, 471 U.S. 386 (1985).
208. *See Terry*, 392 U.S. 1.
209. *See* Gatewood, *supra* note 34 and accompanying text.
210. *See* United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring in judgment) ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical.").

C. Equilibrium Effect of the Mosaic Theory

Professor Orin S. Kerr argues that much of Fourth Amendment jurisprudence is based on what he describes as "equilibrium-adjustment."[211] Professor Kerr describes equilibrium-adjustment as follows:

> Equilibrium-adjustment acts as a correction mechanism. When judges perceive that changing technology or social practice significantly weakens police power to enforce the law, courts adopt lower Fourth Amendment protections for these new circumstances to help restore the status quo ante. On the other hand, when judges perceive that changing technology or social practice significantly enhances government power, courts embrace higher protections to counter the expansion of government power.[212]

As advanced surveillance and tracking technology have greatly expanded the government's power, adoption of the mosaic theory would coexist with Professor Kerr's view of Fourth Amendment jurisprudence by restoring the past level of Fourth Amendment protections.

Under the current prohibitions of the Fourth Amendment, "relatively short-term monitoring of a person's movements on public streets"[213] would be permitted by law enforcement officials having probable cause or reasonable suspicion.[214] Likewise, the use of many other investigatory surveillance techniques to collect and store limited information, presumably to yield sufficient information necessary to secure a warrant, would also be permitted so long as they do not involve a trespass or invade a constitutionally protected area.[215] It is unclear under current constitutional proscriptions how much information can be collected and stored or how long the government may investigate an individual using enhanced surveillance technology.[216] Implementing the mosaic theory to these kinds of Fourth Amendment issues will force the government to make these practical assessments regarding how much and how long or risk having evidence excluded if we assume that the appropriate remedy for a Fourth Amendment violation under the mosaic theory would be the exclusion of the evidence

---

211. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 487–88 (2011).

212. *Id.*

213. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in judgment).

214. *Id. See also* United States v. Knotts, 460 U.S. 276, 281–82 (1983) (discussing the reasonable privacy expectations of individuals in specific situations).

215. *See Gatewood, supra* note 34 and accompanying text.

216. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring in judgment) ("We need not identify with precision the point at which the tracking of this vehicle became a search . . . ."). Likewise, Justice Sotomayor opined that short-term GPS monitoring would "require particular attention" from the Court. *See id.* at 955 (Sotomayor, J., concurring). *See also* United States v. Maynard, 615 F.3d 544, 558–63 (D.C. Cir. 2010) ("It is one thing for a passerby to observe or even to follow someone during a single journey . . . . It is another thing entirely for that stranger to pick up the scent again the next day and the day after that . . . .").

gathered in violation thereof.[217] This assessment will necessarily include an assessment by the government as to the scope of the mosaic theory's reach, including whether or not too much information is being collected and stored or whether or not enhanced tracking surveillance is too long, thereby violating the Fourth Amendment under the mosaic theory. This assessment mirrors the practical considerations that protected Fourth Amendment rights in the past. Prior to modern digital technology, law enforcement officials routinely had to make critical assessments as to how much manpower, how much time, and how many resources they would or could devote to a giving suspect. In making this assessment, no doubt decisions had to be made regarding the potential of obtaining sufficient evidence to meet the probable cause standard. Those suspects that were of limited value most likely received less attention in terms of manpower, time, and resources, thus preserving a degree of privacy as a practical matter, while higher-valued suspects received the bulk of the resources. But even then, the degree of privacy intrusion was still limited by practical considerations that included how much time to devote and how much information could physically be collected.[218] These practical limitations are exactly what protected Fourth Amendment rights in an earlier age. The advent of advanced technology has changed the landscape of "dragnet type"[219] surveillance from something that was "difficult and costly"[220] to something "relatively easy and cheap."[221] The goal of the mosaic theory would be to force law enforcement to make critical decisions regarding the use of such technology instead of using it indiscriminately without concern to privacy implications. In cases where law enforcement officials are unsure whether particular surveillance activity would fall outside the ambient of the mosaic theory, then law enforcement would have the option of seeking independent judicial review and securing a warrant, which, after all, is the point of the Fourth Amendment.[222] As a result, law enforcement is free to pursue its investigation in any practical matter it deems fit, keeping in mind

217. Professor Orin S. Kerr questions whether mosaic search violations should trigger the exclusionary rule because the cost of the exclusionary rule would outweigh it benefits. *See* Kerr, *supra* note 21, at 340–43.

218. *See Jones*, 132 S. Ct. at 963 (Alito, J., concurring in judgment) ("Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken.").

219. *See Knotts*, 460 U.S. at 284 ("[I]f such dragnet-type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.").

220. *Jones*, 132 S. Ct. at 963 (Alito, J., concurring in judgment).

221. *Id.* at 963–64.

222. *See* Johnson v. United States, 333 U.S. 10, 13–14 (1948) ("The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn

that abuses of technology could result in violations of the Fourth Amendment. This resulting effect makes the mosaic theory the great equalizer. Thus, what practical considerations did for Fourth Amendment privacy rights in the pre-computer age, the mosaic theory will do for privacy rights in the wake of advanced technology.

Nevertheless, the question that still remains is why the onus should be on the government, rather than the courts or legislature, to determine the scope of the mosaic theory's reach. In other words, why should not the courts or legislature provide specific guidance to law enforcement on the degree of permissible intrusion that will be permitted by the use of specific technology? The simple answer is that the courts and legislature cannot keep up with the speed of technology.[223] There is no fix-all law that will address all current and future technological advances. By not articulating specific standards in terms of how much information is too much or how long is too long to conduct surveillance, the courts are free to address each new technological advance on a case-by-case basis to determine if the necessary mosaic has been created. Law enforcement and privacy will best be served and preserved if the government is forced to make critical decisions regarding the use and abuse of advanced technology.

V. CONCLUSION

Justice Alito said it best: "[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[224] It is simply that in everyday life, we reasonably expect even in public, certain facts concerning our daily comings and goings will remain private, not because we intend for them to be private (in most instances) but because we do not expect that any one person would be privy to all of our day's events.[225] Implementing the mosaic theory, despite all of the criti-

by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.").

223. *See* Eleanor Birrell, *Technology and the Fourth Amendment: Balancing Law Enforcement with Individual Privacy* 1, 1 (May 20, 2007) (final project for Computer Science, Harvard University), *available at* http://www.eecs.harvard.edu/cs199r/fp/Eleanor.pdf ("One of the reasons for the imbalance between privacy and law enforcement is the lengthy gap between the availability of a new technology and the passage of regulations (either legal or judicial) governing its use. Without any legal or judicial restrictions, law enforcement agencies are free to take advantage of new technologies for years, potentially violating privacy of American citizens.").

224. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in judgment).

225. *See* Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV 119, 134 (2002) (suggesting that because people do not expect to be followed from place to place, there is some measure of privacy expected in one's public movements).

cism raised regarding its application, will help preserve the practical guarantees of the Fourth Amendment by restoring practical limitations and by balancing the government's interest in investigating crime and society's interest in maintaining privacy in and out of the public eye. The mosaic theory comports to our real world expectations of privacy much better than the idea that what a person knowingly exposes to the public cannot also be subject to a reasonable expectation of privacy. It also preserves a degree of public privacy in the face of advanced technology without completely undermining law enforcement's efforts to investigate and prevent crime.