THE MOSAIC THEORY OF THE FOURTH AMENDMENT

Orin S. Kerr*

110 Michigan Law Review (forthcoming 2012).

Abstract

In the Supreme Court's recent decision on GPS surveillance, United States v. Jones (2012), *five Justices authored or joined concurring opinions that applied a new approach to interpreting Fourth Amendment protection. Before* Jones*, Fourth Amendment decisions have always evaluated each step of an investigation individually.* Jones *introduced what we might call a "mosaic theory" of the Fourth Amendment, by which courts evaluate a collective sequence of government activity as an aggregated whole to consider whether the sequence amounts to a search.*

This article considers the implications of a mosaic theory of the Fourth Amendment. It explores the choices and puzzles that a mosaic theory would raise, and it analyzes the merits of the proposed new method of Fourth Amendment analysis. The article makes three major points. First, the mosaic theory represents a dramatic departure from the basic building block of existing Fourth Amendment doctrine. Second, adopting the mosaic theory would require courts to answer a long list of novel and challenging questions. Third, courts should reject the theory and retain the traditional sequential approach to Fourth Amendment analysis. The mosaic approach reflects legitimate concerns, but implementing it would be exceedingly difficult in light of rapid technological change. Courts can better respond to the concerns animating the mosaic theory within the traditional parameters of the sequential approach to Fourth Amendment analysis.

* Professor, George Washington University Law School. Thanks to Will Baude, David Pozen, Daniel Solove, Paul Ohm, Marc Blitz, and Steve Leckar for comments on an earlier draft. This is a June 10, 2012 draft.

Electronic copy available at: http://ssrn.com/abstract=2032821

Table of Contents

Electronic copy available at: http://ssrn.com/abstract=2032821

Introduction

The Fourth Amendment prohibits unreasonable searches and seizures,[1] and the most challenging and important threshold question asks what counts as a Fourth Amendment "search."[2] Identifying Fourth Amendments searches traditionally has required following police action sequentially.[3] If no individual step counts as a search, then the Fourth Amendment is not triggered. No Fourth Amendment violation can occur.

In *United States v. Maynard*,[4] the D.C. Circuit introduced a different approach that I will call the "mosaic theory" of the Fourth Amendment.[5] Under the mosaic theory, searches can be defined collectively as a sequence of discrete steps rather than as individual steps.[6] Identifying Fourth Amendment searches requires analyzing police actions over time as a collective "mosaic" of surveillance; the mosaic can count as a collective Fourth Amendment search even though the individual steps taken in isolation do not.[7] The D.C. Circuit applied that test in *Maynard* to GPS surveillance of a car. The court held that GPS surveillance of a car's location over 28 days aggregates into so much surveillance that the collective sequence triggers Fourth Amendment protection.[8]

When the Supreme Court reviewed *Maynard* in *United States v. Jones,*[9] two concurring opinions signed or joined by five Justices endorsed some form of the D.C. Circuit's mosaic theory.[10] 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 Justices clearly echoed the basic reasoning of the D.C. Circuit in concluding that long-term GPS monitoring of a car

---

[1] U.S. Const. Amend. IV.

[2] *See* Katz v. United States, 389 U.S. 347 (1967).

[3] *See* Section 1.A., *infra*.

[4] 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

[5] I first used this label in a blog post published on the day the *Maynard* decision was handed down. *See* Orin Kerr, *D.C. Circuit Introduces "Mosaic Theory" Of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, http://volokh.com/2010/08/06/ d-c-circuit-introduces- mosaic- theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search/ (August 6, 2010). Other labels are possible, but for the sake of consistency I will adhere to that term.

[6] *Id.* at 562 n.*.

[7] *Maynard*, 615 F.3d 544, 566 (D.C. Cir. 2010).

[8] *Id.*

[9] 132 S. Ct. 945 (2012).

[10] *See* Section 2.B., *infra*.

Electronic copy available at: http://ssrn.com/abstract=2032821

counts as a search even though short-term monitoring does not.[11] Justice Sotomayor's separate concurrence also voiced support for the mosaic approach. [12]

The concurring opinions in *Jones* raise the intriguing possibility that a majority of the Supreme Court is ready to endorse a new mosaic theory of Fourth Amendment protection. That prospect invites lower courts to consider whether the mosaic theory is viable and if so how it should be applied. A handful of courts have already begun to do so in the short time since the Court handed down *Jones*, with mixed results so far.[13] Law enforcement is paying close attention as well. Soon after *Jones*, the FBI's General Counsel informed a law school audience that the mosaic opinions in *Jones* were causing significant turmoil inside the FBI.[14]

The mosaic opinions in *Jones* raise fundamental questions about the future of Fourth Amendment law. What might a mosaic theory mean? What challenges does it entail? Should lower courts eagerly adopt such a method, or do its risks outweigh its benefits? And when the mosaic theory eventually works its way back up to the Supreme Court, should the Court embrace it as a valid theory or reject it as misguided?

This Article considers the consequences of possible judicial adoption of a mosaic theory. It provides a guide to the new approach that maps out possible futures for the mosaic theory, illuminating its nature and detailing the ways in which its implementation raises questions that courts will need to answer.[15] It also evaluates the merits of the mosaic approach and considers whether judges should accept the invitation to adopt the approach in the future.

---

[11] *Id.* at 963-64 (Alito, J., concurring in the judgment). Justice Alito's opinion was joined by Justices Ginsburg, Breyer, and Kagan.

[12] *Id.* at 956 (Sotomayor, J., concurring).

[13] *Compare* United States v. Graham, __ F. Supp. 2d __, 2012 WL 691531 (D. Md. March 01, 2012) (rejecting the mosaic theory for collection of cell-site data) *with* Montana State Fund v. Simms, __ P.3d __, 2012 WL 293460 (Mont. Feb. 1, 2012) (Nelson, J., specially concurring) (suggesting that the mosaic theory should apply to public camera surveillance).

[14] *See* Ariane DeVogue, *Supreme Court Ruling Prompts FBI to Turn Off 3,000 Tracking Devices*, March 7, 2011, available at http://news.yahoo.com/supreme-court-ruling-prompts-fbi-turn-off-3-154046722--abc-news.html

[15] A few student notes and online journal articles have touched on the mosaic theory in the wake of *Maynard*, although none have addressed its operation and merits in detail. Examples of such scholarship that has touched on the theory includes Priscilla J. Smith, Nabiha Syed, David Thaw, & Albert Wong, *When Machines Are Watching: How Warrantless Use Of GPS Surveillance Technology Violates The Fourth Amendment Right Against Unreasonable Searches*, 121 Yale L.J. Online 177, 201 (2011); Justin P. Webb , Note, *Car-ving Out Notions Of Privacy: The Impact Of GPS Tracking And Why Maynard Is A Move In The Right Direction,* 95 Marq. L. Rev. 751 (2011-12); Erin Smith Dennis, Note, *A Mosaic Shield: Maynard, The Fourth Amendment, And Privacy Rights In The Digital Age*, 33 Cardozo L. Rev. 737 (2011).

This article makes three points. First, the mosaic theory is a major departure from the traditional mode of Fourth Amendment analysis. The current structure of Fourth Amendment doctrine hinges on what I will call a "sequential approach." The sequential approach considers whether police conduct is a search in isolation, taking a snapshot of each discrete step and assessing whether that discrete step at that discrete time constitutes a search. This analytical method forms the foundation of existing Fourth Amendment doctrine, ranging from the threshold question of what the Fourth Amendment regulates to constitutional reasonableness and remedies. By aggregating conduct rather than looking to discrete steps, the mosaic theory offers a fundamental challenge to current Fourth Amendment law.

Second, implementing the mosaic theory would require courts to answer an extensive list of difficult and novel questions. Severing the Fourth Amendment from the sequential approach requires courts to start afresh with a new building block of Fourth Amendment analysis. For example, what is the standard for the mosaic? How should courts aggregate conduct to know when a sufficient mosaic has been created? Which techniques should fall within the mosaic approach? Should mosaic searches require a warrant? If so, how can mosaic warrants satisfy the particularity requirement? Should the exclusionary rule apply to violations of the mosaic search doctrine? Who has standing to challenge mosaic searches? Adopting a mosaic theory will require courts to answer all of these questions and more.

Third, as a normative matter, the Supreme Court should reject the mosaic theory. The mosaic approach is animated by legitimate concerns: It aims to maintain the balance of Fourth Amendment protection as technology changes, a method I have elsewhere called "equilibrium adjustment."[16] But it aims to achieve this reasonable goal in a peculiar way. By rejecting the building block of the sequential approach, the mosaic theory would be very difficult to administer coherently. Even if courts could develop answers to the many questions the theory presents, doing so would take many years – by which time the technologies regulated by the theory would be obsolete. The mosaic theory also would deter statutory privacy regulations and force judges to consider questions that they are poorly equipped to answer. If courts must broaden Fourth Amendment rules in response to new technologies, the better approach is to rule that certain steps are always searches. The model should be the Supreme Court's famous decision in *Katz v. United States*,[17] not the concurring opinions in *Jones*.

---

[16] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476 (2011).

[17] 389 U.S. 347 (1967).

This article proceeds in four parts. Part I introduces the sequential approach that forms the basis for existing Fourth Amendment doctrine. Part II provides a close analysis of the D.C. Circuit and Supreme Court decisions on the mosaic theory in *Maynard* and *Jones*. Part III catalogs and considers the many difficult issues that courts would need to answer to implement the mosaic theory. Finally, Part IV argues that courts should reject mosaic theory and retain the traditional sequential approach to interpreting the Fourth Amendment.

I. The Sequential Approach to the Fourth Amendment

This section explains how the sequential approach to Fourth Amendment analysis forms the basic building block of modern Fourth Amendment doctrine. It begins by introducing the sequential approach, and it then examines the three basic stages of Fourth Amendment analysis: First, what is a search; second, when is a search unreasonable and therefore unconstitutional; and third, when does an unconstitutional search justify a remedy.

(A) Sequential Analysis in Search and Seizure Law

Fourth Amendment analysis traditionally has followed what I will call the sequential approach: To analyze whether government action constitutes a Fourth Amendment search or seizure, courts must take a snapshot of the act and assess it in isolation. The "step-by-step analysis is inherent"[18] in evaluating Fourth Amendment claims. This does not mean that searches or seizures happen instantaneously. An officer might search a home for a few hours, and then seize evidence found inside for the duration of the investigation. But a frame-by-frame analysis of the scene governs the analysis. As the Supreme Court has explained, courts focus on each "particular governmental invasion of a citizen's personal security,"[19] starting with the "initial" step and then separately analyzing the "subsequent" steps.[20]

Consider a few examples. If an officer inserts a key into the door of a residence and then opens the door to enter, a reviewing court will first consider the act of inserting the key and then analyze the distinct act of opening the door.[21] If an officer sees expensive stereo equipment in an apartment, moves it to see the serial number, and then records the serial number, a court will treat moving the equipment as distinct from recording

[18] United States v. Beaudoin, 362 F.3d 60, 70-71 (1st Cir. 2004).
[19] Terry v. Ohio, 392 U.S. 1, 19 (1968).
[20] *See* United States v. *Dionisio*, 410 U.S. 1, 8-9 (1973).
[21] *See* United States v. Moses, 540 F.3d 263, 272 (4th Cir. 2008).

the numbers.[22] If an officer sees suspects preparing for a robbery, stops them, and pats them down for weapons, the court will consider the viewing, the stopping, and the patting down as distinct acts that must be analyzed separately.[23] Each step counts as its own Fourth Amendment event and is evaluated independently of the others.

The sequential approach is not merely a minor aspect of Fourth Amendment doctrine. Rather, it forms the basic building block of existing search and seizure law. The remainder of this section explains how the basic structure of existing Fourth Amendment law rests on the sequential approach. It starts with the threshold question of what is a search, then turns to constitutional reasonableness, ad concludes with Fourth Amendment remedies.

(B) The Search Inquiry Under a Sequential Approach

The Supreme Court's established methods for identifying when a Fourth Amendment search occurs reflects the sequential approach. From the 1960s until the Supreme Court's recent *Jones* case, the search inquiry was governed by the "reasonable expectation of privacy" test introduced in Justice Harlan's famous concurring opinion in *Katz*.[24] Although the phrase "reasonable expectation of privacy" is notoriously murky, much of the Supreme Court's caselaw on the reasonable expectation of privacy test can be understood as distinguishing between inside and outside surveillance. Conduct violates a reasonable expectation of privacy test when a government actor breaks into a private enclosed space,[25] such as a home,[26] a car,[27] a package,[28] or a person's pockets.[29] The entrance into the private space exposes the contents of the private space, and the search occurs at the moment of exposure.[30] In contrast, conduct does not violate a reasonable expectation of privacy test when it merely observes the outside of property,[31] when it observes what as been exposed to the public,[32] or when it occurs in public spaces where any citizen may travel.[33]

---

[22] Arizona v. Hicks, 480 U.S. 321 (1987).

[23] *See* Terry v. Ohio, 392 U.S. 1, 17-31 (1968).

[24] *See* Smith v. Maryland, 442 U.S. 735, 739-40 (1979). The Supreme Court's decision in *Jones* explains that this is not the only test, *see* 132 S. Ct. at 953, but it remains the critical test for purposes of the mosaic theory.

[25] *See, e.g.*, Silverman v. United States, 365 U.S. 505, 511 (1961) ("At the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.").

[26] *See id.*

[27] United States v. Ross, 456 U.S. 798, 822 (1982).

[28] *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 114 (1984).

[29] Minnesota v. Dickerson, 508 U.S. 366 (1993).

[30] Cf. United States v. Karo, 468 U.S. 705, 712 (1984) ("It is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence.").

[31] New York v. Class, 475 U.S. 106 (1986)

The sequential approach forms the basic elementary unit of analysis in this traditional approach to the reasonable expectation of privacy test. To know if a search has occurred, courts ask if the government's conduct has crossed the boundary from outside to inside. So long as the government has stayed outside and learned no information about what is inside, no search has occurred.[34] The discrete step of crossing the boundary from outside to inside triggers the Fourth Amendment and counts as a search. A search occurs when the police obtain information about what is hidden inside a private space, whether it is by squeezing a duffle bag to learn its contents[35] or directing a thermal imaging device at a suspect's home to lean its temperature.[36]

The sequential approach also applies to the trespass approach to the Fourth Amendment search doctrine revived in *Jones*. Under *Jones*, a Fourth Amendment search occurs when government actors trespass onto persons, houses, papers and effects with intent to obtain information.[37] The sequential approach naturally matches this traditional doctrine. A search occurs at the moment of the trespass, and it lasts for the period of the trespass. Identifying when a search occurs therefore requires watching the government conduct frame-by-frame and asking when the conduct triggers a trespass.

(C) Constitutional Reasonableness Under the Sequential approach

The sequential approach also proves fundamental to the next inquiry: Whether the conduct amounting to a search is constitutionally "reasonable." Over time, the Supreme Court has offered two different approaches to reasonableness. In the middle of the 20th Century, the Court frequently treated reasonableness as requiring a warrant unless a special exception to the warrant requirement applied.[38] More recently the court has changed emphasis: Reasonableness now is understood as requiring a balancing of interests, which may require a warrant but may require less

---

[32] Katz, 389 U.S. at 361 (Harlan, J., concurring) (stating that "objects, activities, or statements" that a person "exposes to the plain view of outsiders" do not receive Fourth Amendment protection).

[33] See Kyllo v. United States, 533 U.S. 27, 32 (2001).

[34] See, e.g., United States v. Knotts, 460 U.S. 276, 281-82 (1983).

[35] Bond v. United States, 529 U.S. 334 (2000).

[36] Kyllo v. United States, 533 U.S. 27, 32 (2001).

[37] *See Jones*, 132 S. Ct. at 951, 951 n.5.

[38] *See e.g.,* United States v. Jeffers, 342 U.S. 48, 51 (1951) ("Over and again this Court has emphasized that the mandate of the Amendment requires adherence to judicial processes. Only where incident to a valid arrest, or in exceptional circumstances, may an exemption lie, and then the burden is on those seeking the exemption to show the need for it.") (internal citations and quotations omitted).

regulation or even none.[39] Generally speaking, modern Supreme Court doctrine evaluates whether the government interests advanced by the step outweigh the privacy interests it threatens.[40]

Both approaches rest on the assumption that the step is an isolated act. The isolated nature of the search allows the courts to balance the interests for that specific act and create categories of when different kinds of searches are constitutionally reasonable. A few common examples from existing caselaw demonstrate the point. Under existing Supreme Court precedent, searching a home ordinarily requires a warrant.[41] Searches of cars implicate a different balancing of interests, however. Because cars are less private than homes, searching a car requires probable cause but no warrant.[42] A pat-down frisk for weapons implicates yet another balancing. The need to protect officers' safety alters the balance so that the police only need specific and articulable facts that a person is armed and dangerous to conduct the frisk. [43]

Special rules apply in special circumstances as well. For example, the need to protect the federal border enables federal agents to routinely search a person and his property at the border or its functional equivalent.[44] The need to stop terror attacks using airplanes alters the balance of interests and allows TSA to screen individuals and their property at the airport without suspicion.[45] The special harms associated with bodily intrusions bar the police from searching the body to retrieve evidence if the intrusion might threaten the person's health, even with a warrant.[46] Such balancing

---

[39] *See, e.g.,* Samson v. California, 547 U.S. 843, 848 (2006) (""Under our general Fourth Amendment approach we examine the totality of the circumstances to determine whether a search is reasonable within the meaning of the Fourth Amendment.. Whether a search is reasonable is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.") (internal citations and quotations omitted).

[40] *See, e.g.,* United States v. Place, 462 U.S. 696, 703 (1983) ("We must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.").

[41] *See* United States v. Karo, 468 U.S. 705, 714-15 (1984) ("At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable. Our cases have not deviated from this basic Fourth Amendment principle. Searches and seizures inside a home without a warrant are presumptively unreasonable absent exigent circumstances.").

[42] *See* California v. Carney, 471 U.S. 386, 392-94 (1985).

[43] *See* Terry v. Ohio, 392 U.S. 1, 8 (1968).

[44] *See* United States v. Flores-Montano, 541 U.S. 149 (2004).

[45] *See* Electronic Privacy Information Center v. U.S. Dept. of Homeland Sec., 653 F.3d 1, 10-11 (D.C. Cir. 2011).

[46] *See* Winston v. Lee, 470 U.S. 753 (1984).

acts presuppose that each search is a discrete act, triggering a particular balance for that specific set of facts.

The sequential approach also forms the foundation for the warrant requirement. The purpose of the warrant requirement is to ban unlimited searches that allow investigators to go anywhere and search for any kind of evidence.[47] To curb this abuse, the Fourth Amendment's warrant clause has a particularity requirement: Warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized."[48] The particularly requirement limits searches by requiring them to occur in a particular place and to look for specific evidence, such as a search of 123 Main Street for marijuana.[49] Here the sequential approach has obvious force: The particularity requirement rests on the premise that searches are discrete things that can occur in discrete places to find discrete items.

(D) Constitutional Remedies Under the Sequential Approach

When courts declare government conduct an unreasonable search in violation of the Fourth Amendment, courts next must determine the proper remedy. Here, too, the law generally reflects a sequential method of analysis.

Consider the causation principles generally required for Fourth Amendment liability. Remedies apply only if the unconstitutional act caused the discovery of a specific piece of evidence.[50] Establishing causation requires examining two questions. First, was the unconstitutional act a "but for" cause of the discovery of the evidence? Second, was the unconstitutional act a proximate cause of the discovery of the evidence? In the context of the exclusionary rule, the "but for" causation test is known as the "inevitable discovery" and "independent source" doctrines. The proximate cause inquiry takes the form of the colorfully-labeled "fruit of the poisonous tree" doctrine.[51] Similar concepts govern remedies in the context of civil damages, although courts use the traditional labels of causation analysis.[52]

This analysis is naturally tailored to the sequential approach. Deciding whether an influence caused a particular result requires a specific definition of the influence. Identifying whether a particular fact counts as a proximate cause of a result requires identification of the specific fact, permitting an evaluation of how much the fact aided in causing the result.

---

[47] *See* Maryland v. Garrison, 480 U. S. 79, 84 (1987).

[48] U.S. Const. Amend. IV.

[49] Maryland v. Garrison, 480 U. S. 79, 84 (1987).

[50] *See* Hudson v. Michigan, 547 U.S. 586, 590-94 (2006).

[51] *See generally* Wong Sun v. United States, 371 U.S. 471 (1963).

[52] In the civil setting, courts have used similar concepts but under the traditional causation labels, using concepts like intervening causes and events that break the chain of causation. *See, e.g.*, Hector v. Watt, 235 F.3d 154, 161-62 (3d. Cir. 2000).

The same is true with the Fourth Amendment's standing inquiry, which requires the defendant who seeks relief to show that his own rights were violated.[53] Establishing standing generally requires pointing to a particular act in a particular time and place that counts as a search. Courts can then determine if the movant had a sufficient connection to the place searched at that time and place to establish standing.[54]

II. Maynard/Jones *and the Introduction of the Mosaic Theory*

The sequential approach to interpreting the Fourth Amendment has a critical implication: If conduct does not count as a search or seizure, the Fourth Amendment does not regulate it at all. This feature enables investigators to engage in conduct outside Fourth Amendment protection. But now consider the role of computers. Computers excel at repeating processes, and they can do so at ever-faster speeds and at ever-lower prices. The introduction of new high-speed computers poses a challenge to the sequential approach: If certain surveillance practices fall entirely outside the Fourth Amendment, what stops the police from programming computers to conduct that surveillance repeatedly, for a long time, against anyone, for any reason?

Statutory privacy protections provide one answer. Congress has often enacted privacy statutes that regulate in the absence of Fourth Amendment protection.[55] The privacy statutes generally do not codify "full" Fourth Amendment protections such as warrant requirements and the exclusionary rule, but they do require some justification before the government can engage in particular practices that may lead to abuses.[56] Although statutes provide one answer, some may seek a constitutional solution, especially when Congress has not acted. The question is, does the Fourth Amendment have anything to say about limiting government investigations for computerized conduct not regulated under the sequential approach?

Enter the mosaic theory. The theory arose in a recent case, *United States v. Maynard*,[57] later reviewed by the Supreme Court under the name *United States v. Jones*.[58] The mosaic theory requires courts to apply the

---

[53] *See* Rakas v. Illinois, 439 U.S. 128 (1978) Although Rakas warns that the label "standing" is inaccurate, it remains a convenient and widely-used shorthand.

[54] *See id.*

[55] *See, e.g.,* 18 U.S.C. §§ 3121-27, regulating the installation of pen register devices after the Supreme Court declined to do so in Smith v. Maryland, 442 U.S. 735 (1979).

[56] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 596 (2009).

[57] 615 F.3d 544 (D.C. Cir. 2010).

[58] 132 S. Ct. 945 (2012).

Fourth Amendment to government conduct considered as a collective whole rather than as isolated steps. Instead of asking if a particular act is a search, courts consider whether a series of acts that are not searches in isolation amount to a search when considered as a group. In other words, courts consider whether the collective mosaic of individual steps counts as a search.

Understanding the new mosaic theory must begin with a close study of *Maynard/Jones* at both the D.C. Circuit and Supreme Court levels. A close reading of *Maynard/Jones* suggests that five Justices are ready to embrace the new mosaic approach to the Fourth Amendment: Justices Ginsburg, Breyer, Alito, Kagan, and Sotomayor.[59] This section analyzes *Maynard/Jones* with an eye towards how the courts shifted from the sequential approach to the mosaic theory, and what the mosaic theory might mean for the future of Fourth Amendment law.

(A) The Facts of Maynard/Jones

Antoine Jones owned a nightclub in Washington, D.C.[60] Lawrence Maynard served as the nightclub's manager.[61] In 2004, a joint federal and local narcotics task force began to suspect Jones and Maynard of running a massive conspiracy to sell cocaine and crack.[62] A complex two-year investigation followed, and it ultimately led to the discovery of 97 kilograms of cocaine, 1 kilogram of crack, and $850,000 in cash in a stash house run by Jones and Maynard.[63]

Investigators used a wide range of techniques to investigate the case against Jones and Maynard. Investigators obtained wiretap orders and pen register orders to monitor their telephones.[64] They relied on informants to share tips about the conspiracy.[65] They installed a camera at the front door of the nightclub to watch who entered and left.[66] Investigators also obtained search warrants to collect copies of text messages shared among the suspects.[67]

The investigators also used a range of techniques to identify the targets' location. Sophisticated drug dealers generally structure their conspiracies to keep higher-level members away from the contraband.[68] If

---

[59] *Id.* at 963-64 (Alito, J., concurring in the judgment, joined by Justices Ginsburg, Breyer, and Kagan); *id.* at 956 (Sotomayor, J., concurring).

[60] *Maynard*, 615 F.3d at 549.

[61] *Id*. at 549.

[62] *Id.*

[63] *See Jones*, 132 S. Ct. at 948-49.

[64] *Maynard*, 615 F.3d at [].

[65] United States v. Jones, 451 F. Supp. 2d 71, 74 (D.D.C. 2006).

[66] *Jones*, 132 S. Ct. at 948.

[67] *Id.*

[68] This is familiar to fans of the television series *The Wire.*

the police swoop in, they arrest only the low-level dealers who are easy to replace.[69] As leaders of the conspiracy, Jones and Maynard stayed as far away from the drugs as possible. Investigators therefore used three different methods to monitor the physical location of both Jones and Maynard to try to tie them to the conspiracy. The first method of identifying the location of Jones and Maynard was very traditional: The investigators put Jones and Maynard under visual surveillance.[70]

The second method was much more sophisticated. The police knew the number of Jones's cell phone. Cell phones work by connecting to local cellular towers which route communications to and from each phone. Cellular phone service routinely keep records of which towers were used by each account, which can give a rough indicator of the location of the phone -- and by extension, its user. In *Jones*, the investigators and applied for and obtained court orders requiring the cellular provider to provide cell tower information (so called "cell site" data) for Jones's phone.[71] The government obtained several court orders pursuant to the Stored Communications Act,[72] and collected four months' worth of records logging the location of the phone. The government did not seek admission of this evidence at trial, however, and as a result no suppression motion focused on this surveillance on the road to Supreme Court review.[73]

The appellate decisions in *Maynard/Jones* instead focused on the third method of location monitoring, installing a GPS device on Jones's car. Jones drove a Jeep Grand Cherokee that belonged to his wife.[74] Acting cautiously in light of the uncertainty over whether GPS surveillance triggered the Fourth Amendment, officers obtained a warrant from a judge in the District of Columbia authorizing them to install a GPS device on the car Jones drove.[75] The warrant required officers to install the device within 10 days of the warrant's issuance inside the District of Columbia. On the 11th day, the officers installed the GPS device, but did so when they found

---

[69] *See id.*

[70] *Jones*, 132 S. Ct. at 948.

[71] See Defendant's Motion to Suppress Cell Site Data and Memorandum of Points and Authorities in Support Thereof, United States v. Jones, Case No. 05-CR-386(1) (filed March 29, 2012), available at http://legaltimes.typepad.com /files/jones_gps.pdf.

[72] *See* 18 U.S.C. 2703(d) (permitting non-content records from cellular phones to be obtained based on an application establishing specific and articulable facts).

[73] Following the Supreme Court ruling, however, the prosecution is presently attempting to retry Jones in the District Court using the cell-site data. See Defendant's Motion to Suppress Cell Site Data and Memorandum of Points and Authorities in Support Thereof, United States v. Jones, Case No. 05-CR-386(1) (filed March 29, 2012), available at http://legaltimes.typepad.com /files/jones_gps.pdf.

[74] *See, e.g.*, United States v. Johnson, No. CRIM. 05-0386 ESH., 2006 WL 751343 (D.D.C. Mar. 17, 2006) (discussing investigation).

[75] *Jones*, 132 S. Ct. at 948.

the car in a public parking lot in Maryland rather than in the District of Columbia.[76]

The officers used the GPS device to record the location of Jones's car for 28 days. The battery-powered GPS device could record the location of the car within about 50 to 100 feet.[77] Whenever the car was in motion, the GPS device used cell phone technology to broadcast signals of the car's location to a government computer every seven seconds.[78] The device produced over 2,000 pages of location data over 28 days. The location information helped show that Jones's movements were coordinated with those of his co-conspirators, and that he would rendezvous with co-conspirators and visit the stash house in Fort Washington, Maryland, where the drugs and cash were found.[79]

At trial, the prosecution attempted to admit records from the GPS evidence to show that Jones was involved in the conspiracy. Jones moved to suppress the GPS evidence. District Judge Huvelle agreed that any evidence indicating the car was inside Jones's garage had been obtained in violation of the Fourth Amendment.[80] Judge Huvelle concluded that the remaining GPS evidence was admissible under *United States v. Knotts*.[81] *Knotts* had permitted the use of a radio beeper located in a car that broadcast the car's location to the police nearby. According to the Supreme Court in *Knotts*, using the radio beeper to follow the location of a car on public roads did not violate a reasonable expectation of privacy:

> A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] traveled over the public streets, he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.[82]

Judge Huvelle reasoned that the same analysis applied to monitoring using a GPS device.[83] Maynard pled guilty, but Jones went to trial. The jury convicted Jones in a retrial after the first trial resulted in a hung jury.[84]

---

[76] *See id.*
[77] *See id.*
[78] *Maynard*, 615 F.3d at [].
[79] *Jones*, 132 S. Ct. at 948-49.
[80] United States v. Jones, 451 F. Supp. 71, 86 (D.D.C. 2006).
[81] 460 U.S. 276 (1983).
[82] *Id.* at 281-82.
[83] United States v. Jones, 451 F. Supp. 71, 86 (D.D.C. 2006).
[84] *Maynard,* 615 F.3d at [].

(b) The D.C. Circuit's Opinion in Maynard

Maynard and Jones appealed their convictions together, although only Jones challenged the GPS evidence used to convict him at trial. Jones argued to the Court of Appeals that *Knotts* was distinguishable because a GPS device was "light years away"[85] from a radio beeper. Far from merely enhancing the senses, the GPS device gathered so much evidence over time that it could create a full picture of a person's life. Quoting a law student note published in the *Boston College Law Review*,[86] Jones argued to the D.C. Circuit that GPS monitoring was so intrusive even in public that it resembled an invasive search:

> Even though one may expect fleeting glances in public, and police should not have to avert their eyes from what they can see in public, one does not thereby expect the targeted aggregation of data a GPS device collects on one's movements, particularly a kind of surveillance the individual can neither detect nor prevent.[87]

The D.C. Circuit affirmed Maynard's conviction but reversed the conviction of Jones on the ground that monitoring the GPS device over 28 days was a Fourth Amendment "search."[88] Judge Douglas Ginsburg reasoned that *Knotts* was inapplicable because *Knotts* had suggested that "dragnet-type law enforcement practices" might trigger "different constitutional principles."[89] They did, Judge Ginsburg reasoned, and a GPS device was just such a "dragnet-type law enforcement practice." *Knotts* therefore did not control.

Once freed from *Knotts*, Judge Ginsburg turned to the "reasonable expectation of privacy" inquiry. Judge Ginsburg relied on a string of cases applying what I have elsewhere called the probabilistic model of Fourth Amendment protection.[90] Under these cases, whether government conduct violates a reasonable expectation of privacy depends in significant part on

---

[85] See Brief of Antoine Jones in D.C. Circuit, available at 2009 WL 3155141.

[86] April A. Otterburg, *GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment*, 46 B.C. L. Rev. 661 (2005).

[87] See Brief of Antoine Jones in D.C. Circuit, available at 2009 WL 3155141 (quoting April A. Otterburg, *GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment*, 46 B.C.L. Rev. 661, 696-97 (2005)).

[88] *Maynard*, 615 F.3d at 556-57.

[89] *Id.* (citing *Knotts*, at 283–84).

[90] *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev. 503, 508-11 (2008).

the likelihood that evidence will be exposed to the public.[91] In Judge Ginsburg's view, these cases indicated that the core question raised by GPS monitoring was the likelihood that the information collected by GPS monitoring was exposed to the public.[92]

Judge Ginsburg's answer to this question redefined the basic unit of Fourth Amendment law. Instead of looking at the likelihood that discrete pieces of GPS information would be exposed to the public, Judge Ginsburg considered whether the entirety of the GPS monitoring over the course of 28 days, *considered as a collective whole,* would be so exposed. In his view, the monitoring over 28 days constituted a "search" because it was extremely unlikely that the public would actually observe the entirety of such movements.[93] Members of the public would surely see discrete parts of it considered in isolation. But it was essentially impossible for any one person to observe the complete set:

> [T]he whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil. 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.[94]

Judge Ginsburg acknowledged that the discrete readings of the GPS device revealed information exposed to the public. But he reasoned that even if each of the individual readings was exposed in a constructive sense -- that is, they were exposed even if no one actually observed them –- the collective entity of the 28 days of surveillance was not so exposed, because the collective sum of 28 days of surveillance revealed more than the sum of its parts. "The difference is not one of degree but of kind," Judge Ginsburg wrote, "for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more.[95] Many non-searches packaged

---

[91] *Id*.
[92] *Maynard*, 615 F.3d at 558.
[93] *Id.*
[94] *Id*. at 560.
[95] *Id*. at 562.

together as a collective entity *became* a search because the individual pieces of the puzzle that seemed small in isolation could be assembled together like a mosaic to reveal the full picture of a person's life.

For precedent, Judge Ginsburg turned to a Freedom of Information Act case, *United States Department of Justice v. Reporters Committee for Freedom of Press*.[96] *Reporters Committee* had held that the FBI had properly refused to disclose "rap sheets" listing the criminal convictions of individuals under an exception to FOIA that applies when the disclosure could reasonably be expected to constitute an invasion of personal privacy. Although individual acts reported on the rap sheets were already public, the Supreme Court reasoned that bringing the information together for easy access made a major difference: "Plainly there 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."[97]

Judge Ginsburg reasoned that the same mosaic principle should apply in the Fourth Amendment setting. The whole was not merely the sum of the parts:

> 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 a 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.[98]

When considered as a collective whole, the monitoring over 28 days therefore constituted a Fourth Amendment search: "prolonged GPS

[96] 489 U.S. 749 (1989).
[97] *Id*. at 764.
[98] *Id.* at 562.

monitoring reveals an intimate picture of the subject's life that he expects no one to have—short perhaps of his spouse."[99] Such an intrusion into private affairs exceeded the intrusions of the kinds of the police practices that the Supreme Court had deemed a search.

Because the Justice Department had not raised the reasonableness of any search below, the D.C. Circuit declined to address whether the search was reasonable and ordered Jones's conviction overturned.[100] The D.C. Circuit denied rehearing over several dissents, including one by Judge Kavanaugh that pointed to an alternative rationale: Perhaps it was the installation of the device, not its use, that was a Fourth Amendment search.[101]

(C) The Supreme Court's Opinions in Jones

The Supreme Court unanimously agreed with the D.C. Circuit that Jones had been the subject of a Fourth Amendment search, although the Justices divided sharply on why.[102] Writing for a five-Justice majority, Justice Scalia's opinion for the Court followed Judge Kavanaugh's suggestion and held that the installation of the GPS device searched Jones's car because it was a trespass on the "effects" of the car.[103] Justice Scalia therefore did not need to reach the mosaic theory adopted below.[104] On the other hand, five Justices wrote or joined opinions that touched on the issue. Their opinions are somewhat cryptic, but they suggest that a majority of the Court is ready to embrace some form of the D.C. Circuit's mosaic theory.

The starting point for considering the mosaic theory at the Supreme Court is Justice Alito's concurrence in the judgment, joined by Justices Ginsburg, Breyer, and Kagan.[105] Most of Justice Alito's concurring opinion criticized the majority's trespass rationale.[106] Near the end, however, Justice Alito turned to how he would have resolved the case. Like the D.C. Circuit, Justice Alito focused on the long-term use of the GPS device rather than its installation.

Justice Alito accepted *United States v. Knotts* as a precedent, but he construed it as limited to "relatively short-term monitoring of a person's movements."[107] According to Justice Alito, the long-term monitoring of the

---

[99] Id. at 563.
[100] *Id.* at 567-68.
[101] *Id.* at 563-64
[102] *See* United States v. Jones, 132 S. Ct. 945 (2012).
[103] *Id*. at 951-54.
[104] *Id.* at 953-54.
[105] *See id*. at 957-64 (Alito, J., concurring in the judgment).
[106] This page numeration refers to the slip opinion, which is available online at http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf (last visited March 6, 2012).
[107] *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment).

car presented a different issue.[108] Justice Alito focused his application of the reasonable expectation of privacy test on expectations of how law enforcement would investigate particular offenses. According to Justice Alito, society has an expectation of how different crimes might be investigated. For most offenses, "society's expectation has been that law enforcement agents and others would not – and indeed, in the main, could not"[109] monitor the location of the suspect's car in such a detailed way. Jones's narcotics conspiracy was such an offense. The same might not be true of an "extraordinary offense[]," [110] Justice Alito warned. For "extraordinary" crimes, such extensive monitoring might be expected based on "previously available techniques." [111] But because the narcotics conspiracy in *Jones* apparently was not "extraordinary," the degree of observation implicated by long-term monitoring exceeded society's expectations and therefore constituted a Fourth Amendment search.

Justice Alito's analysis is cryptic, in part because this section of his opinion cites no authority. At the same time, Justice Alito's concurring opinion in *Jones* echoes the D.C. Circuit's mosaic approach in *Maynard*. Like the D.C. Circuit, Justice Alito concluded that long-term GPS monitoring constituted a search while short-term monitoring did not.[112] More broadly, by shifting the probabilistic inquiry from what a person might expect the public to *see* to what a person might expect the police to *do*, Justice Alito introduced the element of time that is critical to the mosaic approach. Justice Alito analyzed the constitutionality of the monitoring in Jones by asking if the entirety of the monitoring over 28 days exceeded societal expectations. Implicitly, the unit of the search was a collective whole over an extended period of time.

Justice Alito's concurrence in the judgment drew four votes: Justices Alito, Ginsburg, Breyer, and Kagan.[113] Establishing a majority for the mosaic theory requires a fifth vote, which requires consideration of Justice Sotomayor's solo concurring opinion. Justice Sotomayor joined the majority opinion, and she also agreed with Justice Alito that use of a GPS device constituted a search independently of its installation. Justice Sotomayor reasoned that "the unique attributes of GPS monitoring"[114] – its precision, detail, and efficiency – should guide the constitutional analysis of its use:

---

[108] *Id.*
[109] *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment).
[110] *Id.*
[111] *Id.*
[112] *Id.*
[113] *See id.* at 957.
[114] *Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring).

> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. 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.[115]

This passage clearly echoes the mosaic theory. Justice Sotomayor focuses on whether a person has Fourth Amendment rights "in the sum" of their public movements, rather than in individual movements. Second, Justice Sotomayor asks whether people reasonably expect that their movements not only will be recorded, but also "aggregated." This is the language of aggregation and sums from the mosaic theory, not of individual acts from the sequential approach.

Importantly, Justice Sotomayor's version of the mosaic theory suggests a different standard than that adopted by Justice Alito. Justice Alito's version of the mosaic looked to whether police action was surprising. It focused on whether the investigation exceeded society's expectations for how the police would investigate a particular crime.[116] In contrast, Justice Sotomayor's approach looks to whether police conduct collected so much information that it enabled the government to learn about a person's private affairs "more or less at will."[117] Despite these differences, both of the concurring opinions in *Jones* look to the collective sum of government action, rather than individual sequential steps, to determine what counts as a Fourth Amendment search. Between the two opinions, five Justices have authored or joined opinions that reflect a mosaic approach.

III. Implementing the Mosaic Theory

The possible adoption of the mosaic theory raises challenging new questions for the future of Fourth Amendment law. On one hand, it is surely true that combining together many pieces of information about a suspect can lead the government to learn intimate details about his life.[118]

---

[115] *Id*. at 956.

[116] *Id.* at 964 (Alito, J., concurring in the judgment).

[117] *See Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring).

[118] *See, e.g.,* David E. Pozen, *Deep Secrecy*, 62 Stan. L. Rev. 257, 284 (2010) ("As more and more items of information emerge about a secret plan or policy, outsiders will have more and more opportunities to draw inferences across the items and to relate them to

But in the past this was considered good policing rather than cause for alarm: Assembling and analyzing many pieces of information using non-search techniques has been considered necessary to establish sufficient cause to justify legal searches,[119] not a potential unlawful search itself. The very different premises of the mosaic theory open a wide range of new questions for courts to answer.

This section considers the choices that courts must consider if they decide to adopt a mosaic approach. The lesson of this section is that implementing a mosaic theory would require courts to answer a remarkable set of novel and difficult questions. The theory is so different from what has come before that implementing it would requires the creation of what amounts to a parallel set of Fourth Amendment rules. For every settled question of law under the sequential approach, courts would need to reanalyze the framework for the mosaic theory. And, for the most part, the challenge is exponentially more complicated. Under the sequential approach, searches are simple points. Replacing those points with complex aggregates over space and time is akin to introducing *Flatland*'s square to a three dimensional world.[120]

The analysis focuses on four major questions:

1. The Standard Question. The first question is, what is the standard of the mosaic theory? What test determines when a mosaic has been created? The three pro-mosaic opinions in *Maynard/Jones* suggested three different standards, and future courts will have to choose which standard they mean to adopt. Articulating the standard also requires determining what stages of surveillance a mosaic search regulates. Is data collection enough, or is subsequent analysis and use also required? If the latter, what are the constitutional standards for data analysis and disclosure?

2. *The Grouping Question.* The mosaic theory groups non-searches, and asks if the non-searches considered as a group cross the line to become a search. If courts adopt a mosaic theory, they will need to adopt a theory of grouping to explain which non-searches should be grouped to assess whether the group crosses the mosaic line. This requires courts to answer such questions as which surveillance methods prompt a mosaic approach; how and whether to group across surveillance methods; what is the half-life of a past mosaic search; and how to assess the scope of a mosaic.

---

other items of information they possess. Such analytic mosaic-making is a basic precept of intelligence gathering, used by our government to learn about our enemies and by our enemies to learn about us.").

[119] *Cf.* United States v. R. Enterprises, Inc., 498 U.S. 292, 297 (1991) ("The Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists.")

[120] Edwin Abbott, Flatland: A Romance of Many Dimensions (1884).

3. *Constitutional Reasonableness.* The next question is how to analyze the reasonableness of mosaic searches. Mosaic searches do not fit an obvious doctrinal box to determine their reasonableness: The nature of the mosaic is that each mosaic will be different, potentially requiring different kinds of reasonableness analysis for each one. This concern is bolstered by the fact that the mosaic may aggregate across many different kinds of surveillance, each of which will raise its own reasonableness concerns. Courts will have to create a framework for determining the reasonableness of mosaic searches.

4. *Remedies for Mosaic Violations.* The final question is what remedies should apply to unconstitutional mosaic searches. Does the exclusionary rule apply to mosaic searches? If so, does the rule extend over all the mosaic or only the surveillance that crossed the line from non-searches to searches? Who has standing to challenge mosaic searches? How should courts apply remedial limitations such as inevitable discovery given that some parts of the mosaic may have been inevitably discovered and others were not? Also, when should civil remedies be available for mosaic theory violations? Courts will have to craft a new remedial jurisprudence for the new mosaic search.

(A) Identifying the Standard

The first question raised by the potential adoption of a mosaic theory is the proper standard for aggregation. This question divides into two parts: First, identifying the proper reference point for when when a mosaic has been created; and second, identifying the stages of surveillance that the mosaic theory regulates.

(*1) Expectations of What?*

The first question raised by the mosaic theory is what kinds of expectations of privacy the mosaic theory should recognize. The three pro-mosaic opinions in *Maynard/Jones* each suggest a different answer. Justice Alito focused on societal expectations about law enforcement practices.[121] In his view, a search occurs when investigators collect and analyze evidence in a way or to a degree that would surprise members of society.[122] In contrast, Justice Sotomayor offered a more normative standard that looked at government power. In her view, a search occurs when the government can learn details about a person's personal life "more or less at will."[123] In the D.C. Circuit opinion introducing the mosaic, Judge Ginsburg offered yet another standard, focusing on whether the government learned so much more than a stranger would have observed. These three approaches are

[121] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment).
[122] *Id*.
[123] *Id*. at [] (Sotomayor, J., concurring).

quite different. If courts adopt the mosaic theory, which version should they adopt?

Each of the three versions of the mosaic theory offered in *Maynard/Jones* contains its own major ambiguities, as well. Consider Justice Alito's approach, which focus on societal beliefs about police powers.[124] Applying Alito's standard requires courts first to identify what a reasonable person thinks about existing police investigations, and then to identify when an investigation exceeds that expectation in some measured way. This is a difficult task. Perceptions of police powers likely vary quite widely. Different agencies may investigate different cases in different circumstances in different ways. It is not clear how judge can know what a reasonable person expects about police practices in a more general sense under this standard. Now is it clear what kind of deviations from that expectation can trigger the mosaic. Investigations can involve many people using many tools over time, and a reasonably competent defense attorney likely can find at least some aspect of any investigation that might surprise a member of the public in some way. Implementing Justice Alito's approach therefore requires courts to develop a theory of which deviations matter and how much, to cross the line from an expected investigation to a surprising one.

Justice Sotomayor's very different approach is even more ambiguous than Justice Alito's. According to Justice Sotomayor, courts must 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."[125] If taken literally, this language appears to direct courts to first identify a threshold of "more or less at will" for how easily the government can "record and aggregate" information that allows the government to obtain information – what or how much is left certain – about a person's "political and religious beliefs, sexual habits, and so on." Courts must then determine whether the public has the reasonable expectation that this will occur. But what does this mean? Phrases like "and so on" and "more or less at will" do not identify legal standards as much as make suggestions for further inquiry. Adopting Justice Sotomayor's standard would require significant elaboration.

Ambiguities remain if courts use Judge Ginsburg's standard and look to the likelihood that aggregated evidence will be observed by strangers instead of by the police. The police tend to work together as a unit, so a police-focused standard can plausibly look at the police as a collective entity. But strangers can either work in isolation or in a group. This creates significant ambiguity: Is the relevant standard whether the

[124] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment).

[125] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

mosaic exceeds societal expectation of what one single stranger would see? Or is the issue expectations of what all strangers collectively would see? Does it depend on whether the strangers would aggregate and analyze their information? Adopting Judge Ginsburg's standard would require courts to answer such questions.

(2) *The Stages of Surveillance*

The next question is what stages of surveillance the mosaic theory should regulate. Surveillance regimes often involve several stages: First, the acquisition of information; second, the analysis of that information; and third, th1e use or disclosure of that information.[126] Fourth Amendment law traditionally has focused only on the first step, the acquisition of information.[127] The subsequent analysis and use of information has been considered beyond the scope of Fourth Amendment protection. [128]

The mosaic theory may change this. Justice Alito's opinion in *Jones* looked to whether a person reasonably expects others to "secretly monitor *and catalog*"[129] a person's movements. Justice Sotomayor asked "whether people reasonably expect that their movements will be recorded *and aggregated*" [130] in a manner that creates the mosaic. Cataloging and aggregating are verbs that describe analysis, not acquisition.

These phrases suggest that the mosaic theory requires some step beyond the acquisition of evidence. If so, courts will need to determine what kinds of post-acquisition conduct are required to create a mosaic. Imagine the government collects a great deal of mosaic information but never combines it into a single database. Has a mosaic been created? Or imagine the evidence is collected into a database but never analyzed. Does that cross the line? If some analysis is required to trigger the mosaic, what kind of analysis counts? Does any analysis suffice, or is there some

---

[126] Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law*, at 4-5, available at http://www.brookings.edu/~/media/Files/rc/papers/2011/0419_surveillance_laws _kerr/0419_surveillance_law_kerr.pdf

[127] *Id*. at 6, 9-10.

[128] This is true for two reasons. First, if the information collected is not subject to Fourth Amendment protection, then its analysis raises no Fourth Amendment issues. *See, e.g.,* State v. Sloane, 939 A.2d 796 (N.J. 2008) (holding that searching through a database of criminal records is not a Fourth Amendment "search" because the criminal records are matters of public record). Second, even if the information collected was once subject to Fourth Amendment protection, the initial search of that information eliminates a subsequent expectation of privacy. See Illinois v. Andreas, 463 U.S. 765, 771-72 (1983) ("[O]nce the police are lawfully in a position to observe an item firsthand, its owner's privacy interest in that item is lost.").

[129] *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) (emphasis added).

[130] *See id.* at 956 (Sotomayor, J., concurring) (emphasis added).

threshold of sophistication or computational complexity before the mosaic line has been crossed?

Identifying the precise stage regulated by the mosaic theory is particularly important in light of the requirement of state action in Fourth Amendment law. The Fourth Amendment only applies to conduct by the government or its agents.[131] If private parties conduct surveillance, that surveillance cannot constitute a Fourth Amendment search unless the parties acted as agents of the government.[132] Identifying the stages of the mosaic is essential because government agents and private parties can divide surveillance tasks: Private parties need only take over enough of the process to avoid creating a mosaic.

To see this, imagine a private party collects mosaic data without government involvement. Now imagine that the government either asks for this information, obtains a court order compelling the private party to disclose it, or the private party voluntarily discloses the records to the government. Government investigators then analyze the data and use it to identify a suspect's whereabouts or conduct. Does the Fourth Amendment apply if a private party created the data and the government only analyzed it? Does it depend on whether the government compelled the data from the provider or the provider voluntarily disclosed the data to the government? And what if the roles are reversed, and the government collects the data that is then analyzed by a private party? Does the Fourth Amendment apply to the collection without analysis? Shifting from a sequential approach to a mosaic theory requires identifying exactly which steps in the mosaic require government action to trigger Fourth Amendment protections.

(B) The Grouping Problem: Developing a Theory of Aggregation for the Mosaic Search

After courts settle the standard to be used to gauge if a mosaic has been created, the next question is how to solve the grouping problem. The mosaic theory looks at a collective set of points of data collection, and it determines when that set crosses the boundary and triggers a search. Applying this approach requires a theory of grouping—a theory of what should be aggregated and how—to determine what facts to examine to assess when that trigger point has been reached. Three major categories of questions must be considered: first, duration, and how to measure scale; second, which surveillance methods count; and third, how and whether to group across different investigations.

1. Duration and Scale

---

[131] *See* United States v. Jacobsen, 466 U.S. 109, 113-14 (1984).
[132] *See id.*

The first initial grouping question is the most obvious: How long must the tool be used before the relevant mosaic is created? In *Jones*, the GPS device was installed for 28 days. Justice Alito stated that this was "surely"[133] long enough to create a mosaic. But he provided no reason why, and he recognized that "other cases may present more difficult questions."[134] May indeed. If 28 days is too far, how about 21 days? Or 14 days? Or 3.6 days? Where is the line?

Identifying the required time of surveillance only scratches the surface of the problem. Modern technological tools such as GPS devices can be programmed to record at any interval. The ability to program surveillance tools greatly complicates legal standards based on time. To appreciate this, imagine the police use a GPS device that is programmed to turn on and record the location of the car only for one hour a day. For the other 23 hours a day, the device is dormant. If the police monitor that device for 28 days, does that count as 28 days of monitoring? Or is it only 28 hours of monitoring? [135]

Software can be configured to collect data in more complex ways, further complicating the problem. Imagine the device is set to record the location of the car once a month, at midnight on the night of the first day of the month. If the police install the device and use it for one month, they will have only one data point. Should this count as one month of location monitoring, or is it only a single observation? In the language of Justice Alito's opinion, is this "long term" surveillance that is a search or "short term" surveillance that is not a search?

Software also can be configured to combine these techniques. For example, the police might configure a GPS device to record both a single location at midnight one night a month and also one hour a week from 4am to 5am. Assume, for the sake of argument, that the Supreme Court eventually draws the line for *continuous* GPS monitoring at 7 days. How should courts calculate when this monitoring reaches 7 days? Is the configuration of the device irrelevant? Or should courts count hour by hour, with single-location GPS monitoring assigned some sort of time (say, 30 minutes), until they reach a week?

A related question is whether delay makes a difference. Does a mosaic have a half-life, such that the portion of an earlier mosaic fades over time and restarts the mosaic clock? Let's continue with the assumption that

---

[133] *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4–week mark.").

[134] *Id.*

[135] This was true, but unremarked on by the concurring opinions, in *Jones*. The GPS devices in *Jones* were programmed to record location every 15 minutes, and only when the car was moving.

the Supreme Court eventually holds that 7 days of continuous GPS monitoring on a car counts as a search. Imagine the police monitor a suspect for 5 days and then give up and remove the GPS device. A few years later, the police decide to reopen the case, and they install another GPS device and use it for 3 days. Does this count as 8 days of monitoring, such that the mosaic was created and the conduct was a search? Or does this count as 5 days of monitoring in one year and 3 days of monitoring a few years later, neither of which is a search? [136]

The counting problem is exacerbated by the fact that different suspects will act differently at different times. As a result, the amount of private information collected by the surveillance will vary greatly from suspect to suspect. For example, imagine the police know that one suspect rarely uses his car while a second suspect drives several hours a day. The police install GPS devices on both cars for one week, revealing very little about the first suspect and a great deal about the habits of the second. Does the mosaic amount to a search earlier for the second suspect than the first? Or do the days of monitoring accumulate in the same way regardless of how the car is used? Does it matter if the police know these differences before the monitoring occurs? Courts will have to decide whether these differences matter, and if so, if they mater independently of police knowledge or if some police knowledge is required.

2. Which Surveillance Methods Count?

The next question courts will have to answer is which surveillance methods trigger the mosaic theory, and whether and how to group across different methods. The facts of *Maynard/Jones* are illustrative. In *Maynard/Jones*, GPS surveillance was only one tool among several. The government obtained cell phone location records, installed public camera, and watched the suspects in public, all in addition to tapping phones and obtaining text messages.[137] When considering what conduct amounts to a mosaic, which of these different tools are subject to the mosaic inquiry?

Consider a few examples, starting with surveillance methods that monitor location. Should the mosaic theory apply to obtaining records for cell-site location revealed by the suspect's phone to the suspect's cell-phone

[136] An additional complication is that a group of co-conspirators can share a group of cars, and each car can have a surveillance device installed for different periods of time. See, e.g., United States v. Luna–Santillanes, No. 11–20492, 2012 WL 1019601, at *6-*7 (E.D.Mich. Mar.26, 2012) (considering mosaic arguments in a case involving a conspiracy of three narcotics defendants who drove three cars, each of which had GPS installed for different periods of time).

[137] *See* notes [] to [], *supra*.

provider?[138] Should the theory apply if the government uses a drone (an unmanned aerial surveillance vehicle) to monitor the location of the suspect's car? Or cameras that read license plates? If the police send a team of investigators to place the suspect under visual surveillance, should that visual surveillance be subject to the same analysis? How about public camera surveillance, such as that created by closed circuit television cameras or by government investigators monitoring suspects in public?[139] Any of these technologies can be used to identify a suspect's location over time. Courts will need to determine if the mosaic theory applies to each of these techniques, or if some of these techniques are exempt from the analysis.

The next question is whether the mosaic theory only applies to location surveillance. The GPS device in *Jones* broadcast location of a car, and the collective record of the location of the car overtime could allow the government to assemble a picture of what Jones did during that period. But many surveillance tools can assemble a picture of a suspect's life without revealing the person's location. The police might collect records containing every e-mail address a suspect wrote to and every telephone telephone number a suspect dialed. Investigators might monitor every IP address of every website that a suspect visited, or obtain a suspect's credit card statements showing purchases over many months. If the mosaic theory applies to location monitoring, courts will need to consider whether the same theory also extends to other kinds of surveillance.

If the mosaic applies to multiple surveillance methods, an additional question is 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 may require different regulation within the mosaic framework. If the mosaic approach applies to cell-site surveillance, for example, should the required period of surveillance to trigger a search be longer than the period for GPS surveillance because cell-site surveillance is less exact and invasive than GPS surveillance? Or should all techniques subject to a mosaic analysis be treated in the same way?

3. Grouping Across Practices, Officers and Investigations

If the mosaic approach applies to multiple surveillance practices, the next inquiry is how or whether to group across them. Consider *Maynard/Jones*, where the police simultaneously monitored a suspect using

---

[138] *See, e.g.*, United States v. Graham, __ F. Supp. 2d __, 2012 WL 691531 (D. Md. March 01, 2012) (rejecting the mosaic theory for collection of cell-site data).

[139] *See, e.g.*, Montana State Fund v. Simms, __ P.3d __, 2012 WL 293460 (Mont. Feb. 1, 2012) (Nelson, J., specially concurring) (suggesting that the mosaic theory should apply to public camera surveillance).

cell-site tracking, visual surveillance, and GPS monitoring.[140] If the mosaic theory applies to each surveillance method individually, should courts apply the mosaic to each surveillance method in isolation? Or should they ask whether the collective of some or all of these methods amounts to a search?[141] If seven days of continuous GPS monitoring creates a mosaic search, how should courts treat, say, six days of combined monitoring through GPS together with three days of cell-site monitoring and one day of visual monitoring? Does that count as ten days' worth of monitoring, or only six?

Grouping problems also arise across investigations. Because multiple investigations can target the same suspect, courts may need to consider whether the mosaic aggregate across different investigations. Imagine a suspect buys a car that has a GPS device installed on it, and that suspect is under investigation by both federal and state authorities. The state investigators turn on the GPS device, monitor the suspect for five days, and then stop monitoring. A few days later, the federal investigators monitor the suspect for another five days and then stop. If seven days of GPS monitoring constitutes a search, whether a search has occurred depends on whether courts aggregate the days across the two investigations.[142]

(C) The Constitutional Reasonableness of Mosaic Searches

After courts define the standard for the mosaic theory, and then develop a theory of grouping, they must next develop a framework for analyzing the reasonableness of mosaic searches. Recall that under the sequential approach, constitutional reasonableness requires a balancing of interests: Courts weigh the invasiveness of the government conduct against the extent to which it serves legitimate government interests, and then determine how much regulation of that step is needed to ensure that the steps are constitutionally reasonable.[143] For some searches, courts require a warrant based on probable cause.[144] For other steps, they require just probable cause, or just reasonable suspicion, or even no suspicion at all.[145] How should this framework apply to mosaic searches? Should mosaic

---

140

[141] These issues did not come up in *Maynard/Jones* because the government did not seek admission of the cell-site monitoring, and it seems that the visual surveillance did not cover the location information revealed by the GPS device and used at trial.

[142] Different investigations might represent different governments, different agencies of the same government, different parts of the same agency, or a mix of these options. They might know of each other, or they might not.

[143] *See* United States v. Place, 462 U.S. 696, 703 (1983); In re Subpoena Duces Tecum, 228 F.3d 341, 348-49 (4th Cir. 2000).

[144] *See* United States v. Karo, 468 U.S. 705, 719 (1984)

[145] *Compare* California v. Carney, 471 U.S. 386, 392-94 (1985) *with* Terry v. Ohio, 392 U.S. 1, 30 (1968).

searches require search warrants, and if so, how should such warrants be drafted? If courts do not require warrants, what lesser process should be required?

The question is difficult because the reasonableness of searches traditionally has been tied to the location of the place searched and the circumstances in which the search occurred. Searches of homes ordinarily require a warrant.[146] Searches of cars ordinarily require probable cause but no warrant.[147] Limited frisks of persons for weapons require only reasonable suspicion that a suspect is armed and dangerous.[148] And most of these searches can be performed with less or even no suspicion in special circumstances, ranging from searches of probationers and parolees (no suspicion required)[149] to searches under exigent circumstances (general reasonableness required).[150]

Applying these principles to mosaic searches raises novel issues because mosaic searches target a "place" that has never before been regulated under the Fourth Amendment. In *Maynard/Jones*, for example, GPS monitoring collected information about Jones's public location. The Justices agreed that the government conduct constituted a search, but the Justices did not reach the reasonableness of the search because the question was not litigated below.[151] If the Justices had reached the question, the pro-mosaic Justices would have had to decide a question of first impression: What is the reasonableness of a search of public spaces? No court has ever considered the question before *Jones* for the simple reason that public location surveillance has never before been considered a "search."[152]

Several different outcomes seem plausible. Some Fourth Amendment precedents present the warrant requirement as a default and suggest that a specific exception must be articulated for another standard to apply.[153] If courts follow those cases, they might conclude that mosaic searches require a warrant simply because there is no strong reason not to

---

[146] *See Karo*, 468 U.S. at 719.

[147] *See Carney*, 471 U.S. at 392-94.

[148] *See Terry*, 392 U.S. at 8.

[149] *See* Samson v. California, 547 U.S. 843, 843–44 (2006).

[150] *See* Kentucky v. King, 131 S. Ct. 1849, 1858 (2011).

[151] *Maynard*, 615 F.3d at 567.

[152] To be sure, in *Karo*, the Supreme Court did rule that use of a radio beeper to determine the location of property inside a home requires a warrant. But the reason was that the beeper disclosed information about the inside of a home, which traditionally requires a warrant. *See Karo*, 468 U.S. at 718-19.

[153] *See, e.g.,* Katz v. United States, 389 U.S. 347, 357 (1967) (stating that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment --subject only to a few specifically established and well-delineated exceptions").

apply a warrant requirement.[154] Courts also might say that mosaic searches require a warrant because mosaic searches are quite invasive when considered cumulatively, or that the benefit of ex ante judicial review makes a warrant requirement reasonable.[155]

On the other hand, other precedents focus more on the Fourth Amendment's requirement of reasonableness, which might require a warrant but might not.[156] Courts could apply those precedents to conclude that mosaic searches are less invasive than home searches and therefore do not require a warrant. For example, courts might analogize mosaic searches to car searches: Just as persons only have a reduced expectation of privacy in their cars in part because cars are often searched and exposed to public view, justifying less Fourth Amendment protection for cars than homes,[157] perhaps persons have only a reduced expectation of privacy in open spaces that are "searched" by the mosaic.

The reasonableness of mosaic searches becomes particularly complicated if courts conclude that multiple kinds of surveillance practices trigger the mosaic inquiry. If several different methods of surveillance trigger the mosaic theory, courts would need to consider if the reasonableness of a mosaic search is a "one-size-fits-all" question or different kinds of mosaics implicate different reasonableness standards. For example, perhaps GPS mosaic searches are so invasive that they require a warrant, but cell-site mosaic searches -- being less detailed and accurate than GPS mosaic searches -- require only probable cause. Or perhaps mosaic searches operate on a graduated scale, requiring lesser suspicion when they first trigger the mosaic threshold but then requiring greater suspicion and a warrant as the surveillance continues.

Courts will next need to answer what kind of probable cause or reasonable suspicion is required. Probable cause and reasonable suspicion represent levels of probability. But what these standards mean depend on the question, *probability of what*? When the Fourth Amendment requires probable cause to arrest, for example, the probable cause means probable cause to believe a crime has been committed and the suspect committed

---

[154] *Cf.* State v. Zahn, --- N.W.2d ----, 2012 WL 862707 at *7 (S.D. 2012) (suggesting that a warrant exception applies to mosaic searches because no exception to the warrant requirement applies).

[155] *See id.* at *8 ("Because the unfettered use of surveillance technology could fundamentally alter the relationship between our government and its citizens, we require oversight by a neutral magistrate.").

[156] *See, e.g.,* Illinois v. McArthur, 531 U.S. 326, 330 (2001) (noting that "the central requirement" of the Fourth Amendment "is one of reasonableness," which has led the Supreme Court to "interpret[] the Amendment as establishing rules and presumptions designed to control conduct of law enforcement officers that may significantly intrude upon privacy interests" that "[s]ometimes . . require warrants" and other times do not).

[157] *See Carney*, 471 U.S. at 392-94.

it.[158] When the Fourth Amendment requires search warrants, however, probable cause means probable cause to believe that evidence or contraband will be found inside the place to be searched.[159] The meaning of probable cause depends on the context, with different kinds of searches and seizures requiring probable cause of different kinds of facts.

That prompts an intriguing question: If mosaic searches require probable cause, then probable cause of what do they require? Do they require probable cause to believe that the location of the suspect is evidence of a crime? Probable cause to believe that the suspect monitored has committed a crime? Some other standard?

A recent opinion by a federal magistrate judge demonstrates the difficulty.[160] Investigators looking for a fugitive applied for a warrant to collect both GPS and cell-site location evidence in an effort to locate the fugitive and prosecute him. The government's application established probable cause to believe the monitoring would help find the fugitive, and that the fugitive was wanted for violations of federal law. The magistrate judge rejected the government's application on the ground that warrants allowed by the Fourth Amendment require probable cause that the location evidence was itself evidence of a crime, not merely that it would help the government find a fugitive.[161] Because the government had provided no reason to think that the fugitive's location was itself evidence of a crime, the Fourth Amendment did not permit the court to issue a warrant.[162]

If courts conclude that mosaic searches require a warrant, they also must answer how courts can satisfy the particularity requirement of the warrant clause in mosaic search cases. The Fourth Amendment states that warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized."[163] But what is the specific "place" to be searched in a mosaic search? By their nature, mosaic searches aggregate across many places. The concept of mosaic searches draws on the fact that they bring together information from many places and instances to create a detailed picture of a suspect's life. The search does not occur in any one place. What is the "place" to be searched, then: The world? Or perhaps the collective places where the suspect happens to go?

The issue is particularly complex if the mosaic theory regulates beyond the collection of evidence to include its analysis and use.[164] Should the "place" where the search takes place include where the analysis and use

---

[158] Warden v. Hayden, 387 U.S. 294 (1967).

[159] *Id.* at 307.

[160] *See* In the Matter of an Application of the United States of America, --- F. Supp. 2d ----, 2011 WL 3423370 (D. Md. 2011).

[161] *See id.* at [].

[162] *Id.* at []

[163] U.S. Const. Amend IV.

[164] See notes [] to [], supra.

occurs, or only where the collection occurs? Similar problems arise with the requirement of particularly describing the "thing" that is "seized." Mosaic searches do not seem to "seize" anything. Rather, they collect information about a person's whereabouts and life. And assuming *something* is seized over the course of a mosaic,[165] how can a warrant describe that thing to be seized with the specificity needed to satisfy the particularity requirement? The question is difficult because the purpose of the requirement is to ensure that searches remain narrow: Searches must be limited to a single place and a hunt for specific evidence.[166] The theory of mosaic searches flips this understanding on its head. Mosaic investigations are deemed searches precisely because they are *not* limited. Reconciling the mosaic search theory and the particularity requirement may prove quite difficult.[167]

(D) Remedies for Mosaic Searches

The final set of questions concerns the scope of remedies for unconstitutional mosaic searches. The first question is whether the exclusionary rule should apply to mosaic search violations; the second question is who has standing to challenge mosaic searches; and the third question considers the scope of the fruit of the poisonous tree and inevitable discovery doctrines.

(*1) Does the Exclusionary Rule Apply?*

---

[165] *Cf. United States v. Freitas*, 800 F.2d 1451, 1455-56 (9th Cir. 1986) (concluding that a warrant rule permitting officers to obtain a warrant to and seize property authorizes the police to obtain a sneak-and-peek because entry into a space "seizes" information about what is inside it).

[166] *See* U.S. Const. Amend. IV.

[167] Courts have encountered somewhat related questions before, although the guidance in those precedents is only modestly helpful. In *United States v. Karo*, 468 U.S. 705 (1984), the Supreme Court suggest that when the police needed to obtain a warrant to use a radio beeper, the place to be searched was "the object into which the beeper is to be placed." *Id*. at 718. This guidance does not answer how particularity applies in the case of the mosaic theory, however, as the mosaic theory applies to the collection of evidence over time rather than the installation of a device. *See Jones*, 132 S. Ct. at [] (Alito, J., concurring in the judgment).

Caselaw on the particularity requirement for roving wiretaps provides another reference point, but it also has substantial limitations. Investigators can obtain roving wiretap orders when suspects frequently change phones; the orders allow the government to monitor phone calls over whatever telephone facilities the suspects use. Although lower courts have upheld the roving wiretap authority, *see, e.g., United States v. Petti*, 973 F.2d 1441 (9th Cir. 1992), roving wiretaps still state the place to be searched: "Only telephone facilities actually used by an identified speaker may be subjected to surveillance." *Id*. at 1445. In other words, the place to be searched is the specific telephone facility where the suspect is placing a phone call. In the case of a mosaic, in contrast, it is axiomatic that the search cannot occur in a single place.

The first significant question is whether mosaic search violations should trigger the exclusionary rule. In *Hudson v. Michigan*,[168] the Supreme Court held that violations of the Fourth Amendment "knock-and-announce" rule do not justify the exclusionary sanction. The knock-and-announce rule generally requires agents executing warrants to first knock on the door and announce their presence, and then wait a "reasonable time" before entering the place to be searched.[169] *Hudson* concluded that suppression for knock-and-announce violations was inappropriate because the costs of the exclusionary rule in that setting outweighed its benefits: The murkiness of exactly what the "reasonable time" standard requires would trigger endless litigation,[170] and it was likely that the combination of civil remedies and the training of professional officers would lead to substantial compliance with the rule even without a suppression remedy.[171]

If courts recognize the mosaic search doctrine, they will need to consider whether mosaic search violations are exempt from the exclusionary rule under *Hudson*. On one hand, courts might plausibly analogize knock-and-announce violations and mosaic search violations. Both standards are murky and would likely draw significant litigation. To the extent civil remedies and professionalism ensure that officers comply with the knock-and-announce rule, the same reasoning might suggest that officers can comply with the mosaic search rules (whatever they turn out to be). On the other hand, courts could distinguish mosaic searches on the ground that they are more directly related to the discovery of evidence to be suppressed. In knock-and-announce cases, the violation and discovery of evidence generally are unrelated. Failing to knock and announce does not change the evidence discovered.[172] In contrast, if investigators use tools that create a mosaic of a suspect, at least some parts of the mosaic are likely to lead to information that could be used in court if it reveals evidence of crime.

If courts reject *Hudson* as a basis for denying an exclusionary remedy for mosaic searches, the good-faith exception to the exclusionary rule may nonetheless substantially narrow its application. The Supreme Court's most recent cases on the good-faith exception indicate that the exclusionary rule does not apply unless an officer acted culpably.[173] Although the cases are not a model of clarity, they seem to indicate that the violation must be intentional, reckless, or grossly negligent to generate the

[168] 547 U. S. 586 (2006).
[169] Wilson v. Arkansas, 514 U. S. 927, 931-932 (1995).
[170] *See Hudson*, 547 U.S. at 597-98.
[171] *See id.* at 598-99
[172] *Hudson*, 547 U.S. at [].
[173] *See Davis*, 131 S. Ct. at 2428.

deterrence that justifies suppression.[174] Otherwise, the violation is one in "good faith" and no exclusionary rule applies.[175] Depending on how courts implement the mosaic theory, a plausible argument exists that the good-faith exception may apply to many types of mosaic searches. If courts cannot specify ex ante with clarity when police conduct aggregates sufficiently to constitute a search, officers may understandably cross the line without personal culpability. Unless the violation is a brazen one, the exclusionary rule may not apply.

Privacy statutes may also limit the scope of the exclusionary rule. Under *Illinois v. Krull*,[176] the exclusionary rule does not apply if officers reasonably rely on statutes that authorize their conduct. State laws regulating GPS surveillance may provide a basis for reasonable reliance:[177] To the extent the scope of the mosaic theory remains unclear, officers who follow statutes regulating GPS surveillance are likely to avoid suppression even courts take a more restrictive view of the GPS surveillance than do the relevant statutes.[178]

(2) Standing to Challenge Mosaic Searches

If the exclusionary rule is available for mosaic search violations, courts will need to determine its scope. The initial question asks who has standing to challenge a mosaic search. Fourth Amendment rights are personal, and individuals can invoke a remedy only if their own rights were violated.[179] The Fourth Amendment standing inquiry arises as an application of the reasonable expectation of privacy test; each person must establish that his or her own reasonable expectation of privacy was violated to have standing to challenge the government's act.[180]

---

[174] *Id.* at 2422 (citing *Herring*, 555 U.S. at 137).

[175] *Id.* at 2427-27.

[176] 480 U.S. 340 (1987).

[177] For example, Minn. Stat. Ann. §§ 626A.35-7 requires the government to obtain a court order to install a mobile tracking device, and it authorizes the surveillance for up to 60 days based on proof of "reason to believe that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation." Minn. Stat. Ann. § 626A.37. This appears to be a lower standard than probable cause. *See* State v. Fakler, 503 N.W.2d 783, 786-87 (Minn. 1993) (analyzing the "reason to believe" standard in the Minnesota state surveillance statutes).

[178] In the short term, the good-faith exception to the exclusionary rule for reliance on binding appellate precedent might also play a role. *See* Davis v. United States, 131 S.Ct. 2419 (2011) (extending the good-faith exception to reliance on binding appellate precedent). Application of *Davis* to mosaic searches is murky, however, as it remains unclear to what extent reliance on the discrete-steps approach counts reliance on binding precedent.

[179] Minnesota v. Carter, 525 U.S. 83, 99 (1998) ("Fourth Amendment rights are personal, and when a person objects to the search of a place and invokes the exclusionary rule, he or she must have the requisite connection to that place.").

[180] Rakas v. Illinois, 439 U.S. 128 (1978).

The difficult question is identifying who has standing to challenge an unlawful mosaic search. Mosaic searches occur over time, and the overall mosaic therefore may monitor different people at different times in different degrees. This creates considerable complexity. To see why, imagine the police have installed a GPS device on Alan's car. Bob steals Alan's car and begins to drive it around town. Bob drives the car for 30 days, and during that time he often gives rides to Charles, Dave, and Elizabeth. Charles gets a ride almost every day; Dave every other day; and Elizabeth only rides in the car twice. The police remotely turn on the GPS device when the car is reported stolen, and they monitor the car for 28 days. We know from *Jones* that five Justices would say that 28 days of GPS monitoring amounts to a search. But who has standing to challenge it?

Does Bob have standing on the ground that his location was monitored for the full 28 days?[181] Or does he lack standing because the stole the car, and therefore has no rights in it?[182] If Bob has standing, what about Charles, Dave, and Elizabeth? Do all three have standing because their location was monitored as part of a broader mosaic search? Or must the standing inquiry look to each individual, requiring an assessment of whether the monitoring of each individual suspect was enough to constitute a mosaic? If the exclusionary rule applies to mosaic searches, courts will need to develop answers to these questions.

(3) Fruit of the Poisonous Tree and Inevitable Discovery

Assuming the exclusionary rule applies and the defendant can challenge the search, the next question is whether the unconstitutional conduct acts as the but-for and proximate cause of the discovery of the relevant evidence, thus justifying its suppression. In the context of the exclusionary rule, these questions arise under the rubric of the "fruit of the poisonous tree" and "inevitable discovery."[183] These doctrines raise puzzling questions for mosaic violations because it is difficult to identify the unconstitutional mosaic act. Is the collective activity over time that creates the mosaic a single unconstitutional act, or is the unconstitutional act only the surveillance that occurred after the monitoring reaches a mosaic?

Consider whether the exclusionary rule applies to the entire mosaic or only some part of the mosaic. To simplify matters, let's use the prior

---

[181] *Cf.* United States v. Hanna, No. 11-20678-CR, 2012 WL 279435 (S.D. Fla. Jan 30, 2012) (holding that only the owner or exclusive user of the car has standing to challenge a mosaic search of its location).

[182] United States v. Caymen, 404 F.3d 1196, 1201 (9th Cir. 2005) (applying general rule that individuals do not have Fourth Amendment rights in property obtained by fraud).

[183] *See* notes [] to [], *supra*.

assumption that seven days of GPS monitoring crosses the line to become a search. If the police monitor a GPS device for ten days, must the entire ten days of monitoring be suppressed? Or should courts only suppress the last three days of monitoring data that occurred after the mosaic point? If the police learn from the location information on day two that the suspect committed a crime, should the evidence from day two be suppressed because it was part of the mosaic, even though the collection of that evidence was not a search when it occurred? Or is the evidence from the second day an inevitable discovery because it would have been discovered if the monitoring had stopped before the amount of monitoring crossed the mosaic threshold?

A related issue arises when investigators use surveillance to locate targets at a particular time rather than develop a picture of their lives over time. Consider a recent case involving a GPS device attached to a car used to transport heroin.[184] Investigators used the GPS tracking to find the car. After finding the car, officers conducted a pretextual traffic stop based on a traffic violation, asked for and obtained consent to search the car, and then retrieved two kilograms of heroin inside.[185] Assuming the GPS device was used long enough to cross the threshold of a search, is the heroin a fruit of the poisonous mosaic search? Or does the exclusionary rule not apply either because the traffic stop and consent dissipate the taint or because the stop was not a product of the mosaic but rather a short-term use of the GPS device? Again, these are difficult questions that courts will have to answer if they embrace a mosaic theory.

IV. The Case Against the Mosaic Theory

The five votes in favor of a mosaic approach in *United States v. Jones*[186] do not establish the theory as a matter of law. The majority opinion in *Jones* failed to adopt the mosaic approach, and it only touched on the mosaic method in passing to express skepticism of it.[187] Even if five votes of the current court are ready to embrace the theory, lower courts must adhere to Supreme Court holdings even when subsequent developments suggest that the Supreme Court would reject those holdings if it reviewed

[184] United States v. Luna–Santillanes, 2012 WL 1019601 (E.D. Mich. March 26, 2012).

[185] See id.

[186] 132 S. Ct. 945 (2012).

[187] *Id.* at 954 (referring to the approach articulated in Justice Alito's opinion as "thorny," "vexing," and "a novelty," and asking, "What of a 2–day monitoring of a suspected purveyor of stolen electronics? Or of a 6–month monitoring of a suspected terrorist?").

them.[188] For now, then, the sequential approach remains good law. At the same time, the concurring opinions in *Jones* invite lower courts to consider embracing some form of the mosaic approach. Our attention therefore must turn to the normative question: Should courts embrace the mosaic theory? Is the mosaic approach a promising new method of Fourth Amendment interpretation, or is it a mistake that should be avoided?

This section argues that courts should reject the mosaic theory. The better course is to retain the traditional sequential approach to Fourth Amendment analysis. The mosaic theory aims at a reasonable goal. Changing technology can outpace the assumptions of existing precedents, and courts may need to tweak prior doctrine to restore the balance of privacy protection from an earlier age. I have called this process "equilibrium adjustment,"[189] and it is a longstanding method of interpreting the Fourth Amendment. But the mosaic theory aims to achieve this goal in a very peculiar way.

The mosaic theory amounts to an awkward half-measure. Under the sequential approach, courts traditionally have two options when deciding how to regulate police conduct. They can say that the conduct is *never* a Fourth Amendment search, but that legislatures can regulate the conduct by enacting statutory protections; or else they can say that conduct is *always* a Fourth Amendment search. The mosaic theory offers a vague middle ground as a third option. The theory allows courts to say that techniques are *sometimes* a search. They are not searches when grouped in some ways (when no mosaic exists) but become searches when grouped in other ways (when the mosaic line is crossed).

Identifying those contexts is extremely difficult, however, such that the challenges of the method outweigh its alleged benefits. As Part III showed, implementing the mosaic theory raises a large number of novel and complex questions that courts would need to answer. It is hard to see how courts can answer all these questions coherently. Indeed, even the proponents of the mosaic approach don't seem to have any idea how it should apply.[190]

Rather than jump headfirst into this morass, the wiser course is to retain the two options presented under the sequential approach. This does not mean that courts must allow technology to erode Fourth Amendment privacy. It means that if courts must expand Fourth Amendment privacy

---

[188] See Rodriguez de Quijas v. Shearson /American Express, Inc., 490 U.S. 477, 484 (1989) ("If a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the Court of Appeals should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions.")

[189] *See* Kerr, *supra* note [].

[190] *See* notes [] to [], *infra*.

protections in response to new technologies they should deem the conduct always a search, not merely sometimes a search. The model for this approach is the most famous Fourth Amendment case of them all: *Katz v. United States*.[191]

(A) The Mosaic Theory As Equilibrium-Adjustment

In a recent article,[192] I argued that much of modern Fourth Amendment doctrine reflects the principle of equilibrium-adjustment. When technology and social practice change in ways that substantially threaten government power to solve crimes, courts often respond by loosening Fourth Amendment rules to restore the prior level of investigatory power. On the other hand, when technology and social practice considerably expand government power, courts respond by strengthening Fourth Amendment rules to attempt to restore the prior level of constitutional protection. Judges interpret the Fourth Amendment in response major technological changes much like a driver trying to maintain speed on hilly terrain: They add gas when climbing uphill but lay off the pedal on the downslopes.[193]

The mosaic theory of the Fourth Amendment fits nicely into this framework. Computerization enables extremely fast repetition of surveillance practices. If a computer can do something, it can do that thing many times in a split second. Computers also have a previously unimaginable capacity to aggregate and analyze whatever information investigators collect. The mosaic theory attempts to restore the balance of power by disabling the government's ability to rely on what computerization enables. As Justice Alito noted in *Jones*, surveillance in "the pre-computer age" [194] was necessarily limited, while computers changed massive-scale monitoring from something "impractical" to something "relatively easy and cheap."[195] Such new powers "may alter the relationship between citizen and government," [196] Justice Sotomayor worried, resulting in "a tool so amenable to misuse"[197] that the Fourth Amendment needed to step in.

The mosaic theory aims to restore the balance of police power by labeling the government's enhanced powers as searches. If investigators use new tools in modest ways consistent with earlier government capacities,

---

[191] 389 U.S. 347 (1967).

[192] *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment,* 125 Harv. L. Rev. 476 (2011).

[193] *See id.* at 487-90 (explaining the process of equilibrium-adjustment).

[194] *Jones*, 132 S. Ct. at 963 (Alito, J., concurring in the judgment).

[195] *Id*. at 964.

[196] *Id*. at 956 (Sotomayor, J., concurring) (quoting United States v. Cuevas–Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

[197] *Id.*

the use of the tools remains outside the scope of Fourth Amendment protection. But as the government exploits the new powers provided by the new tools, the surveillance eventually goes too far, upsets the earlier balance, and subjects the government's conduct to Fourth Amendment oversight.

(*B) The Case Against the Mosaic Theory*

The critical question is whether the mosaic theory offers a desirable version of equilibrium-adjustment. Although the mosaic theory derives from an admirable goal, I believe it is a troubling approach that courts should reject. The mosaic theory should be rejected for three reasons. First, the theory raises so many novel and puzzling new questions that it is difficult if not impossible to administer effectively as technology changes. Second, the mosaic theory rests on a probabilistic conception of the reasonable expectation of privacy test that is ill-suited to regulate the new technologies that the mosaic theory has been created to address. And third, the theory interferes with the role of statutory protections, which are more effective ways to regulate surveillance practices outside the sequential approach.

To be clear, rejecting the mosaic theory does not mean that courts must cease to engage in equilibrium-adjustment or accept that new technologies must diminish the role of the Fourth Amendment. Courts can and should continue to engage in equilibrium-adjustment using the sequential approach. The model for this approach is *Katz v. United States*, which expanded Fourth Amendment protections in light of new technologies within the sequential framework.

(1) The Mosaic Theory Would Be Very Difficult to Administer

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. Because the mosaic theory departs dramatically from existing doctrine, implementing it would require the creation of a new set of Fourth Amendment rules – a mosaic parallel to the sequential precedents that exist today. The problem is not only the number of questions, but their difficulty. Many of the questions raised in Part III of this article are genuine puzzles that Fourth Amendment text, principles and history cannot readily answer. Judges should be reluctant to open the legal equivalent of Pandora's Box.

It is particularly telling that not even the proponents of the mosaic theory have yet proposed answers for how the theory should be applied. For example, a group of Fellows at Yale's Information Society Project who endorse the mosaic approach simply dismissed the conceptual difficulties of its implementation on the ground that answering such puzzles is "why we

have judges."[198] A pro-mosaic amicus brief in *Jones* signed by several prominent legal academics was similarly nonresponsive. Although the mosaic approach requires "tough decisions" to be made, the brief noted, courts have encountered difficult questions elsewhere in Fourth Amendment law.[199] While one can admire such confidence in the capabilities of the judiciary, it would provide more comfort if proponents of the mosaic theory would at least be willing to venture guesses as to how it should apply.

The challenge of answering the questions raised by the mosaic theory has particular force because the theory attempts to regulate use of changing technologies. Law enforcement implementation of new technologies can occur very quickly, while judicial resolution of difficult constitutional questions occurs at a more glacial pace. As a result, the constantly-evolving nature of surveillance practices could lead new questions to arise faster than courts can settle them. Old practices would likely be obsolete by the time the courts resolved how to address them, and the newest surveillance practices would arrive and their legality would remain unknown. Like Lucy and Ethel trying to package candy on the ever-faster conveyor belt,[200] the mosaic theory could place judges in the uncomfortable position of trying to settle a wide range of novel questions for technologies that are changing faster than the courts can resolve how to regulate them.

Consider the changes in location-identifying technologies in the last three decades. Thirty years ago, the latest in police technologies to track location was the primitive radio beeper seen in *Knotts*. But radio beepers have gone the way of the 8-track tape. Today the police have new tools at their disposal that were unknown in the *Knotts* era, ranging from GPS devices to cell-site records to license–plate cameras. This rapid pace of technological change creates major difficulties for courts trying to apply the mosaic theory: If the technological facts of the mosaic change quickly over time, any effort to answer the many difficult questions raised by the mosaic theory will become quickly outdated. Courts may devise answers to the many questions discussed in Part III, but by the time they do the relevant technology is likely to have gone the way of the radio beeper.

---

[198] *See* Priscilla J. Smith, Nabiha Syed, David Thaw, & Albert Wong, *When Machines Are Watching: How Warrantless Use Of GPS Surveillance Technology Violates The Fourth Amendment Right Against Unreasonable Searches*, 121 Yale L.J. Online 177, 201 (2011).

[199] See Amicus Curiae Brief of Yale Law School Information Society Project Scholars and Other Experts in the Law of Privacy and Technology in Support of the Respondent, *United States v. Jones*, at 25, available at 2011 WL 4614429. The scholars who signed onto this brief included Daniel Solove, Paul Ohm, Danielle Citron, Christopher Slobogin, Susan Freiwald, Renee Hutchins, Chris Hoofnagle, and Stephen Henderson.

[200] *See* I Love Lucy, Job Switching (original air date Sept 15, 1952).

(2) Probabilistic Approaches to the "Reasonable Expectation of Privacy" Test Are Ill-Suited To Regulate Technological Surveillance

The third problem with the mosaic theory is that most formulations of it are based on a probabilistic approach to the reasonable expectation of privacy test that proves ill-suited to regulate technological surveillance practices. Supreme Court decisions have utilized several different inquiries for what makes an expectation of privacy constitutionally reasonable.[201] In some cases the Court has looked to what a reasonable person would perceive as likely;[202] in other cases the Court has looked to whether the particular kind information obtained is worthy of protection;[203] in some cases the Court has looked to whether the government violated some legal norm such as property in obtaining the information;[204] and in other cases the Court has simply considered whether theconduct should be regulated by the Fourth Amendmnet as a matter of policy.[205] Use of these multiple inquiries (what I have called "models") of Fourth Amendment protection allows the Court to adopt different approaches in different contexts, ideally selecting the model that best identifies the need for regulation in that particular setting.[206]

For the most part, formulations of the mosaic theory rest on the first of these approaches – what a reasonable person would see as likely. I have called this the probabilistic approach to Fourth Amendment protection,[207] as it rests on a notion of the probability of privacy protection. The more likely it is that a person's will maintain their privacy, the more likely it is that government conduct defeating that expectation counts a search. Under this model, the Fourth Amendment guards against surprises. The paradigmatic example is *Bond v. United States*,[208] which involved government agents manipulating the duffel bag of a bus passenger to identify a wrapped brick of drugs inside it. A bus passenger expects other passengers to handle his bag but not "feel the bag in an exploratory manner,"[209] the Court held, so the exploratory feel violated a reasonable expectation of privacy. Both Judge Ginsburg and Justice Alito authored mosaic opinions that rely on such probabilistic reasoning. Judge Ginsburg deemed long-term GPS monitoring a search because no stranger could conduct the same level of monitoring as a GPS device. Justice Alito reached the same result on the

---

[201] *See* Kerr, *Four Models*, *supra* note 90.
[202] See id. at 508-512.
[203] *See id.* at 512-16.
[204] *See id.* at 516-19.
[205] *See id*. at 519-22.
[206] *See id.* at 543-48.
[207] *See* Kerr, *Four Models*, *supra* note 90, at 508-12.
[208] 529 U.S. 334 (2000).
[209] *Id*. at 339.

grounds that a reasonable person would not expect the police to obtain so much information.

The probabilistic approach presents a poor choice to regulate technological surveillance because most individuals lack a reliable way to gauge the likelihood of technological surveillance methods. The probabilistic expectation of privacy applied in *Bond* relied on widespread and repeated personal experience. Bus passengers learn the social practices of bus travel by observing it first-hand. In contrast, estimating the frequency of technological surveillance practices is essentially impossible for most people (and most judges). Surveillance practices tend to be hidden, and few understand the relevant technologies. Some people will guess that privacy invasions are common, and others will guess that they are rare. But none will know the truth, which makes such probabilistic beliefs a poor basis for Fourth Amendment regulation.

Consider the so-called "CSI effect,"[210] by which jurors in routine criminal cases expect prosecutors to introduce evidence collected using high-tech investigatory tools featured on popular television dramas such as *Law & Order* and *CSI*. The CSI effect suggests that members of the public derive their expectations of police practices in large part from entertaining but largely fictional television shows. Resting Fourth Amendment doctrine on such malleable expectations seems a curious choice. A hit show featuring hard-working officers with high-tech investigatory tools could cut back Fourth Amendment protection, as it would suggest that even a very invasive investigation is commonplace. On the other hand, a new show featuring lazy or incompetent officers might expand Fourth Amendment protection, as a thorough investigation will come to exceed societal expectations. It is hard to see why Fourth Amendment protections should track such poorly-informed beliefs.

Nor does Supreme Court doctrine require it. To the contrary, the Supreme Court has generally avoided applying the probabilistic model to government surveillance practices.[211] The Court has relied instead on other models that provide more stable ways to regulate government surveillance practices.[212] Courts should follow that lead, continuing to focus on the models of the reasonable expectation of privacy test that do not rely on probabilistic reasoning.

---

[210] *See* Simon A. Cole & Rachel Dioso-Villa, *Investigating The 'CSI Effect' Effect: Media And Litigation Crisis In Criminal Law*, 61 Stan. L. Rev. 1335 (2009).

[211] *See* United States v. Sparks, 750 F. Supp. 2d 384, 392 (D. Mass. 2010) ("Rather than using a probabilistic approach to determine reasonable expectations of privacy, in the context of governmental use of new technologies, the Supreme Court repeatedly has focused on whether the nature of the information revealed is private and thus worthy of constitutional protection").

[212] *Id.*

(3) The Mosaic Theory Could Interfere With More Effective Statutory Protections

A third difficulty with the mosaic theory is that it may interfere with the development of statutory privacy laws. As I have explained in another article[213] – and as Justice Alito suggested in his concurring opinion in *Jones*[214] – Congress has significant institutional advantages over the courts in trying to regulate privacy in new technologies. Congress can act quickly and hold hearings and consider expert opinion.[215] Congress can adopt half-measures that don't fit easily in constitutional doctrine and can draw arbitrary lines.[216] And if Congress errs or facts change, Congress can amend its prior handiwork relatively easilt.[217] Congress can also regulate using sunset provisions that force the legislature to revisit the question in light of intervening experience.[218] For these reasons, legislative privacy laws have considerable institutional advantages over the products of the comparatively slow and less-informed judicial process.

The mosaic approach could interfere with statutory solutions in two ways. First, the theory might discourage legislative action by fostering a sense that the courts have occupied the field.[219] When courts hear a controversial privacy case but rule that the Fourth Amendment does not apply, the judicial "no" identifies a problem for the legislature to address: The absence of judicial regulation invites legislative action. Prominent examples include the Right to Financial Privacy Act,[220] passed in response to *United States v. Miller*;[221] the Pen Register statute,[222] passed in response to *Smith v. Maryland*;[223] and the Privacy Protection Act,[224] passed in response to *Zurcher v. Stanford Daily*.[225] In all three instances, Congress responded to a Fourth Amendment ruling allowing a controversial investigatory practice by creating statutory protections that limit use of the

---

[213] *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev 801, 855-57 (2004).

[214] *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) (citing Kerr, *supra* note 213, at 805-06).

[215] *See* Kerr, *supra* note 213, at 870, 881-82.

[216] *See id.* at 871-72.

[217] *See id.*

[218]

[219] *See* Kerr, *supra* note 213, at 855-57.

[220] Pub. L. 95-630, 92 Stat. 3697 (1978), codified at 12 U.S.C. §§ 3401-22.

[221] 425 U.S. 435 (1976).

[222] 18 U.S.C. §§ 3121-27.

[223] 442 U.S. 735 (1979).

[224] 42 U.S.C. § 2000aa.

[225] 436 U.S. 547 (1978).

practice without imposing a universal warrant requirement.[226] The possibility of mosaic protection complicates the legislative picture because mosaic protections can overlap with possible statutory solutions and therefore render the case for statutory protection much less apparent.[227]

The two concurring opinions in *Jones* can be read as hinting at another possible interaction between the mosaic theory and statutory protections: Perhaps the mosaic theory operates only when no statutory protection exists, such that enactment of statutory protections disables the mosaic theory.[228] If so, the mosaic theory would encourage statutory

---

[226] See, e.g., H.R. Rep. No. 1383, 95th Cong., 2d Sess. 1978, 1978 U.S.C.C.A.N. 9273, 9306 (discussing bills to create statutory right over financial records in response to *Miller*).

[227] This is just a prediction, and the novelty of the mosaic approach makes it difficult to prove. One very modest piece of evidence might be the Congressional action on location privacy before and after *Jones*. In the months leading up to the *Jones* decision, several prominent bills were introduced in Congress to regulate GPS surveillance. In June 2011, Senators Franken and Blumenthal introduced the Location Privacy Protection Act of 2011, S.1223, 112th Cong. (Jun. 16, 2011), and Senator Wyden introduced the Geolocational Privacy and Surveillance Act, S.1212, 112th Cong. (Jun. 15, 2011). In the months following *Jones*, however, those bills appear to be stalled and no other bills have been introduced to date. Of course, one cannot draw much in the way of conclusions from such sparse evidence.

[228] It is important to avoid the academic trap of reading too much into the minutiae and penumbras of Supreme Court opinions. Academics can find deep meaning where no Justice intended it. With that said, Justice Alito introduces his mosaic solution in *Jones* by explaining that it is "[t]he best that we can do" in light of the fact that "to date, . . . Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes." Jones, 132 S. Ct. at 964 (Alito, J., concurring in the judgment). This statement could be interpreted in two ways. On one hand, perhaps it merely means that Justice Alito had to apply the Fourth Amendment because no statutes exist that could allow the Court to decide the legality of the government's conduct without reaching the constitutional question. Under this interpretation, the "best that we can do" language merely reflects the principle of constitutional avoidance.

On the other hand, perhaps the "best that we can do" language means that the existence of privacy statutes disables the mosaic approach, or at least the possibility of an exclusionary remedy. *Cf.* Illinois v. Krull, 480 U.S. 340 (1987) (holding that the exclusionary rule does not apply when an officer reasonably relies on a statute authorizing investigatory conduct later ruled in violation of the Fourth Amendment). This latter interpretation is bolstered somewhat by the fact that even the widespread adoption of GPS statutes likely would not provide a basis for constitutional avoidance in *Jones*, at least outside the context of *Krull*'s good-faith exception. The federal agents in *Jones* would not be bound by a state GPS surveillance statute under the Supremacy Clause, and even a federal privacy statute could only resolve the *Jones* case to the extent it included a statutory suppression remedy.

Justice Sotomayor makes a somewhat similar suggestion in her statement that in applying the Fourth Amendment, she would "consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse[.]" *Id.* at 956 (Sotomayor, J., concurring). This seems to suggest that oversight

protections rather than discourage it. But this possibility raises its own set of complex set of puzzles. For example, how many statutory protections suffice? At the time of *Jones*, a few state legislatures had already enacted GPS privacy laws.[229] A few state supreme courts had regulated GPS monitoring under state constitutions.[230] More states and the federal government were likely to enact such protections in the future. If protections outside the Fourth Amendment end the need for Fourth Amendment protection, how many statutes and state constitutional decisions must be enacted before they are sufficient?

A related puzzle is how much protection such statutes must provide. If *any* statutory protection disables the mosaic, then legislatures can enact the most modest and toothless protection and that will suffice. The mosaic threat will be entirely procedural: Legislatures will need to check the box of establishing statutory protection to avoid a judicially-enforced mosaic. On the other hand, if courts have to assess whether the statutes are sufficiently protective to address the kind of concerns that the mosaic theory addresses, then achieving that standard will be extremely difficult: For reasons I have explained in depth elsewhere, facial review of privacy statutes to determine if they are sufficiently protective to satisfy a general Fourth Amendment standard would trigger its own rather daunting interpretive challenges.[231]

(C) The Mosaic Theory as A Halfway Measure and the Katz *Example*

Rejecting the mosaic theory does not mean that judges must sit idly by as advancing technology diminishes the role of the Fourth Amendment. Under the sequential approach, can engage in equilibrium-adjustment within the context of a binary choice. Judges can label government conduct a non-search, and thereby leave it at most to statutory regulation, or else they can label it a search and subject it to constitutional regulation. Rejecting the mosaic theory allows this process to continue. It simply leaves out the mosaic theory's effort to introduce a middle-ground third option that amounts to an awkward halfway measure.

The mosaic theory provides a halfway-measure because it leaves sequential precedents partially in place. It leaves practices unregulated in some unspecified short-term context, and then flips the switch and holds the government action a search only when grouped together in some broader or longer-term context. Consider the use of GPS devices in *Maynard*/*Jones*. In

---

from a coordinate branch such as Congress might lead her to reach a different interpretation of the Fourth Amendment.

[229] *See, e.g.*, Minn. Stat. § 626A.37; Fla. Stat. § 934.06.

[230] *See, e.g.*, State v. Jackson, 76 P.3d 217, 263-64 (Wash. 2003).

[231] *See* Orin S. Kerr, *Congress, The Courts, and New Technologies: A Response To Professor Solove*, 74 Fordham L. Rev. 779, 787-90 (2005)

United States v. Knotts,[232] the Court had held that use of a government location device to monitor the location of a car on public thoroughfares was never a search.[233] In his mosaic concurrence in *Jones*, Justice Alito reaffirmed the *Knotts* precedent but limited it to "relatively short-term monitoring of a person's movements on public streets."[234] Under this approach, *Knotts* was still good law -- at least up to a point. Justice Alito's mosaic opinion offered an attempted middle ground between retaining *Knotts* in its entirety or simply overturning it.

Although renouncing the mosaic theory would eliminate the middle-ground, it allow judges to continue to engage in equilibrium-adjustment by expanding what constitutes a search. The proper model is *Katz v. United States*,[235] perhaps the most famous of all Fourth Amendment decisions. *Katz* expanded the scope of what constitutes a search by replacing the constitutionally-protected area formulation with something broader. Under *Katz*, bugging and wiretapping that had been beyond Fourth Amendment protection were brought inside that protection to account for the new world of telephone communications. Notably, the *Katz* Court did not say that short-term bugging was permitted but that long-term bugging became a search at some unspecified point. Instead, the Court followed the traditional sequential approach by holding that *all* bugging of a phone while it was in a person's private use triggered the Fourth Amendment.[236]

Application of the same method to the use of relatively new surveillance techniques such as GPS surveillance suggests that the Court should choose between two basic options. If technology and social practices remain sufficiently stable that the *Knotts/Karo* line properly balances law enforcement power and privacy rights, then courts should adhere to those cases. On the other hand, if changing technology and social practice dramatically expands government power under *Knotts/Karo*, courts can engage in equilibrium-adjustment and overturn *Knotts*. Courts should follow the *Katz* example and engage in equilibrium-adjustment within the confines of the sequential approach.

Conclusion

The concurring opinions in *Jones* invite lower courts to experiment with a new approach to the Fourth Amendment search doctrine. The approach is well-intentioned, in that it aims to restore the balance of Fourth Amendment protection by disabling the new powers created by

[232] 460 U.S. 276, 281-82 (1983).
[233] *Id.*
[234] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment).
[235] 389 U.S. 347 (1967).
[236] *Id.* at [].

computerization of surveillance tools. But despite being well-intentioned, the mosaic theory represents a Pandora's Box that courts should leave closed. The theory raises so many novel and difficult questions that courts would struggle to provide reasonably coherent answers. By the time courts worked through answers for any one technology, the technology would likely be long obsolete. Mosaic protection also could come at a cost of lost statutory protections, and implementing it would require courts to assess probabilities of surveillance that judges are poorly equipped to evaluate. In this case, the game is not worth the candle. The concurring opinions in *Jones* represent an invitation that future courts should decline. Instead of adopting a new mosaic theory, courts should consider the need to engage in equilibrium-adjustment within the confines of the traditional sequential approach.