THE MOSAIC THEORY OF THE FOURTH AMENDMENT

*Orin S. Kerr**

In the Supreme Court's recent decision on GPS surveillance, United States v. Jones, *five justices authored or joined concurring opinions that applied a new approach to interpreting Fourth Amendment protection. Before* Jones, *Fourth Amendment decisions had 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.

TABLE OF CONTENTS

* Fred C. Stevenson Research 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.

INTRODUCTION

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

---

1. U.S. CONST. amend. IV.

2. The issue of what counts as a seizure is comparatively simple, and it therefore has received little scholarly attention. Seizures require governmental assertion of control, so a seizure of property occurs when the government meaningfully interferes with a person's possessory interest. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

3. *See infra* Section I.A.

In *United States v. Maynard*,[4] the D.C. Circuit introduced a different approach, which could be called a "mosaic theory" of the Fourth Amendment.[5] Under the mosaic theory, searches can be analyzed as a collective sequence of 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 twenty-eight 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] concurring opinions signed or joined by five of the 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 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 five-justice 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 begun to do so in the short time since the Court handed down *Jones*, with mixed results so far.[13] Law enforcement is

---

4. 615 F.3d 544 (D.C. Cir.), *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*, VOLOKH CONSPIRACY (Aug. 6, 2010, 2:46 PM), http://volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search/. Other labels are possible, but for the sake of consistency I will adhere to that term.

6. *Maynard*, 615 F.3d at 562 n.*.

7. *Id.* at 566.

8. *Id.* at 561–62.

9. 132 S. Ct. 945.

10. *See infra* Section II.C.

11. *Jones*, 132 S. Ct. 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) (reasoning that determining whether government behavior constitutes a search requires considering "whether people reasonably expect that their movements will be recorded and aggregated" in such a manner).

13. *Compare* United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012) (rejecting the mosaic theory for collection of cell-site data), *with* Mont. State Fund v. Simms, 270 P.3d 64, 69–72 (Mont. 2012) (Nelson, J., specially concurring) (suggesting that the mosaic theory should apply to public camera surveillance).

paying close attention as well. Soon after *Jones*, the General Counsel of the Federal Bureau of Investigation informed a law school audience that the mosaic opinions in *Jones* were causing significant turmoil inside the FBI.[14]

The mosaic opinions in *Jones* implicate 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 maps out the possible futures of the mosaic theory, and it details how the theory 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 it.

The 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 call a "sequential approach." The sequential approach takes a snapshot of each discrete step and assesses 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 considerations of 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 would compel 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

---

14. *See* Ariane de Vogue, *Supreme Court Ruling Prompts FBI to Turn Off 3,000 Tracking Devices*, YAHOO! NEWS (Mar. 7, 2012), 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 include Priscilla J. Smith et al., *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), http://yalelawjournal.org/images/pdfs/1017.pdf; Erin Smith Dennis, Note, *A Mosaic Shield:* Maynard, *the Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737 (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).

a mosaic theory would require courts to answer all of these questions and more.

Third, as a normative matter, courts 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 raises, doing so would take many years—by which time the technologies regulated by the theory would become obsolete. The mosaic theory would also deter enactment of 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*.

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 the 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 building block of modern Fourth Amendment doctrine. It begins by introducing the sequential approach and 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 call the sequential approach: to analyze whether government action constitutes a Fourth Amendment search or seizure, courts 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

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

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

18. United States v. Beaudoin, 362 F.3d 60, 70–71 (1st Cir. 2004), *vacated sub nom.* Champagne v. United States, 125 S. Ct. 1025 (2005) (mem.).

instantaneously. An officer might search a home for a few hours and then seize evidence found inside for the duration of the investigation. But analyzing whether a search has occurred requires a frame-by-frame dissection of the scene. 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 the number.[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 foundation of existing search and seizure analysis. 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 defining a search, then turns to constitutional reasonableness, and concludes with Fourth Amendment remedies.

B. *The Search Inquiry Under the 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 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 case law on the reasonable expectation of privacy test can be understood as distinguishing between inside and outside surveillance. Conduct violates a reasonable expectation of privacy when a government actor breaks into a private, enclosed

19. Terry v. Ohio, 392 U.S. 1, 19 (1968).

20. *See* United States v. Dionisio, 410 U.S. 1, 8–9 (1973).

21. *E.g.*, United States v. Moses, 540 F.3d 263, 272 (4th Cir. 2008).

22. Arizona v. Hicks, 480 U.S. 321, 324–25 (1987).

23. *See Terry*, 392 U.S. at 18 n.15, 27–30.

24. *See* Smith v. Maryland, 442 U.S. 735, 739–40 (1979). The Supreme Court's decision in *United States v. Jones* explains that this is not the only test, *see* 132 S. Ct. 945, 953–54 (2012), but proponents of the mosaic theory have rooted it solely in this test.

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 when it consists of observing the outside of property,[31] observing what has already been exposed to the public,[32] or observing public spaces where anyone may travel.[33]

The sequential approach forms the basic unit of analysis under this traditional inquiry. To know if a search has occurred, courts ask if the government's conduct has crossed the boundary from outside to inside surveillance. So long as the government has stayed outside and acquired no information about what is inside, no search has occurred.[34] A search only happens when the police learn about what is hidden inside a private space, whether by squeezing a duffle bag to learn its contents[35] or aiming a thermal imaging device at a home to learn its temperature.[36]

The sequential approach also applies to the trespass test revived in *Jones*. Under *Jones*, a Fourth Amendment search occurs when government actors trespass onto persons, houses, papers, or 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 analyzing 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 forms a basic part of the next inquiry: whether searches are constitutionally reasonable. Over time, the Supreme

---

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. *Id.*

27. United States v. Ross, 456 U.S. 798, 807–09, 823–25 (1982).

28. *E.g.*, United States v. Jacobsen, 466 U.S. 109, 114 (1984).

29. Minnesota v. Dickerson, 508 U.S. 366, 378 (1993).

30. *See* United States v. Karo, 468 U.S. 705, 712 (1984) ("[W]e have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment. . . . 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, 114 (1986).

32. Katz v. United States, 389 U.S. 347, 361 (1967) (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. *See* Bond v. United States, 529 U.S. 334, 336–37 (2000).

36. *Kyllo*, 533 U.S. at 34–35.

37. United States v. Jones, 132 S. Ct. 945, 951 n.5 (2012).

Court has offered two different approaches to the reasonableness of searches. In the middle of the twentieth century, the Court generally indicated that searches are reasonable only when the government obtains a valid warrant or a special exception to the warrant requirement applies.[38] More recently, the Court has suggested a different approach. Reasonableness now is understood as requiring a balancing of interests: courts consider whether the government interests advanced by the use of an investigatory technique outweigh the privacy interests that its use threatens.[39] Under this approach, reasonableness may require a warrant but may require less regulation or even no regulation at all.[40]

Both approaches to reasonableness rest on the assumption that searches are readily identifiable acts that occur over readily identifiable periods of time.[41] This allows courts to balance the interests for specific kinds of searches and create categories for when different searches are reasonable. A few examples demonstrate the point. Under existing Supreme Court precedent, searching a home ordinarily requires a warrant.[42] In contrast, searching a car implicates a different balancing of interests and leads to a different

---

38. *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." (citations omitted) (quoting Johnson v. United States, 333 U.S. 10, 14–15 (1948))).

39. *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.").

40. For example, the Court in *Samson v. California* explained the balancing approach as follows:

> "[U]nder our general Fourth Amendment approach" we "examin[e] 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."

547 U.S. 843, 848 (2006) (alterations in original) (citations omitted) (quoting United States v. Knights, 534 U.S. 112, 118–19 (2001)).

41. It is true that searches and seizures both occur over a period of time, and the reasonableness inquiry must be made over that period of time. For example, if an officer enters a home and searches for one hour while a second officer detains the homeowner for two hours, the search will occur for one hour while the seizure will last for two hours. But the fact that searches and seizures occur over time does not mean that they reject the sequential approach or implicate a "mosaic." Their existence and duration are clear as they occur, and do not require the ex post aggregation and analysis of non-searches.

42. In *United States v. Karo*, the Court stated as follows:

> 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.

468 U.S. 705, 714–15 (1984).

rule: because cars are less private than homes, searching a car requires probable cause but no warrant.[43] A pat-down frisk for weapons implicates yet another balancing. The need to protect officers' safety alters the balance so that the police need only specific and articulable facts that a person is armed and dangerous in order to conduct the frisk.[44]

Special rules apply in special circumstances as well. For example, the government's need to protect the federal border enables federal agents to routinely search a person and his property at the border or its functional equivalent.[45] The need to stop terror attacks allows the Transportation Security Administration ("TSA") to screen individuals and their property at the airport without suspicion.[46] On the other hand, particularly intrusive searches receive heightened protection. For example, the police cannot search a person's body to retrieve evidence if that intrusion might threaten the person's health, even if they have a warrant.[47] In each of these cases, the analysis presupposes that a search is a readily identifiable act that allows courts to analyze the strength of the interests in play when the government commits that kind of act.

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.[48] To curb this abuse, the Warrant Clause includes a particularity requirement: warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized."[49] The particularity 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.[50] Here the sequential approach has obvious force: the particularity requirement rests on the premise that searches are identifiable acts that occur in identifiable places to find identifiable evidence.

D. *Constitutional Remedies Under the Sequential Approach*

Fourth Amendment law also reflects a sequential method of analysis at the remedies stage. 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.[51] Establishing causation requires examining two questions. First, was the unconstitutional act a

---

43. *See* California v. Carney, 471 U.S. 386, 392–94 (1985).

44. *See* Terry v. Ohio, 392 U.S. 1, 31 (1968).

45. *See* United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004).

46. *See* Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec., 653 F.3d 1, 10–11 (D.C. Cir.), *reh'g en banc denied*, 653 F.3d 1 (D.C. Cir. 2011).

47. *See* Winston v. Lee, 470 U.S. 753, 766 (1985).

48. *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987).

49. U.S. CONST. amend. IV.

50. *See Garrison*, 480 U.S. at 84.

51. *See* Hudson v. Michigan, 547 U.S. 586, 590–94 (2006).

"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 consists of the "inevitable discovery" and "independent source" doctrines. The proximate cause inquiry takes the form of the colorfully labeled "fruit of the poisonous tree" doctrine.[52] Similar concepts govern remedies in the context of civil damages, although courts use the traditional labels of causation analysis.[53]

This causal 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 identifying the specific fact, which then permits an evaluation of how much that fact contributed to the result. 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.[54] 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 to establish standing.[55]

II. *MAYNARD/JONES* AND THE INTRODUCTION OF THE MOSAIC THEORY

The mosaic theory poses a fundamental challenge to the sequential approach. The theory first arose in a recent case, *United States v. Maynard*,[56] later reviewed by the Supreme Court under the name *United States v. Jones*.[57] The mosaic theory requires courts to apply the Fourth Amendment search doctrine to government conduct as a collective whole rather than in isolated steps. Instead of asking if a particular act is a search, the mosaic theory asks whether a series of acts that are not searches in isolation amount to a search when considered as a group. The mosaic theory is therefore premised on aggregation: it considers whether a set of nonsearches aggregated together amount to a search because their collection and subsequent analysis creates a revealing mosaic.

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,

---

52. *See* Wong Sun v. United States, 371 U.S. 471, 484–88 (1963).

53. In the civil setting, courts have used similar concepts but under traditional causation labels such as intervening causes and events that break the chain of causation. *See, e.g.*, Hector v. Watt, 235 F.3d 154, 160–61 (3d Cir. 2000).

54. *See* Rakas v. Illinois, 439 U.S. 128, 133–34 (1978). Although *Rakas* warns that the label "standing" is inaccurate, it remains a convenient and widely used shorthand.

55. *See id.*

56. 615 F.3d 544 (D.C. Cir. 2010).

57. 132 S. Ct. 945 (2012).

Alito, Kagan, and Sotomayor.[58] The next Section analyzes *Maynard/Jones* with an eye toward understanding how the analysis in *Maynard/Jones* shifted the framework for analyzing Fourth Amendment searches from the sequential approach to the mosaic theory. It then considers 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.[59] Lawrence Maynard served as the nightclub's manager.[60] In 2004, a joint federal and local narcotics task force began to suspect Jones and Maynard of orchestrating a massive conspiracy to sell cocaine and crack.[61] A complex two-year investigation followed and 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.[62]

Investigators used a wide range of techniques to develop the case against Jones and Maynard. They obtained wiretap orders and pen register orders to monitor the suspects' telephones,[63] and they relied on informants to share tips about the conspiracy.[64] They also installed a camera at the front door of the nightclub to watch who entered and left.[65] Additionally, investigators obtained search warrants to collect copies of text messages shared among the suspects.[66]

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.[67] That way, if the police swoop in, they will find and arrest only low-level dealers who are easy to replace.[68] 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

---

58. *Jones*, 132 S. Ct. at 963–64 (Alito, J., concurring in the judgment); *id.* at 956 (Sotomayor, J., concurring).

59. *Maynard*, 615 F.3d at 549.

60. *Id.*

61. *Id.*

62. *See Jones*, 132 S. Ct. at 948–49.

63. United States v. Jones, 451 F. Supp. 2d 71, 74 (D.D.C. 2006), *aff'd in part, rev'd in part sub nom.* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

64. *Id.*

65. *Jones*, 132 S. Ct. at 948.

66. *Jones*, 451 F. Supp. 2d at 74.

67. This may be familiar to fans of the television series *The Wire* (HBO television broadcast).

68. *See id.*

of Jones and Maynard was very traditional: the investigators put Jones and Maynard under visual surveillance.[69]

The second method was more sophisticated. The police knew Jones's cell phone number. Cell phones work by connecting to local cell towers, which route communications. Because cell phone providers routinely keep records of which towers were used by each account, the government can obtain cell phone records that act as a rough kind of location device. Most people carry their phones: the location of a suspect's phone tells the police the location of the suspect. In *Maynard/Jones*, investigators applied for and obtained court orders requiring Jones's cellular provider to provide cell tower information (called "cell-site" data) for Jones's phone.[70] The government obtained several court orders pursuant to the Stored Communications Act[71] 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.[72]

The appellate decisions in *Maynard/Jones* focused on the third method of location monitoring: use of a GPS device installed on Jones's car. Jones drove a Jeep Grand Cherokee that belonged to his wife.[73] Officers obtained a warrant from a judge in the District of Columbia authorizing them to install a GPS device on the car.[74] At the time, no legal authority indicated that a warrant was necessary. Although precedents were sparse, and the D.C. courts had not spoken on the issue, other federal courts had ruled that the Fourth Amendment did not apply in such circumstances.[75] The agents obtained a warrant nonetheless, perhaps recognizing that the Supreme Court had not yet settled the issue.[76] Having proceeded cautiously in light of legal uncertainty, however, the agents then blundered in executing the warrant. The warrant required officers to install the device inside the District of Columbia within ten days of the warrant's issuance. The agents did not install the GPS device until the eleventh day when the car happened to be at a public parking lot in Maryland.[77]

---

69. *Jones*, 132 S. Ct. at 948.

70. *See* Defendant's Motion to Suppress Cell Site Data & Memorandum of Points & Authorities in Support Thereof at 1–3, United States v. Jones, No. 05-CR-386(1) (ESH) (D.D.C. Mar. 29, 2012) [hereinafter Defendant's Motion to Suppress], *available at* http://legaltimes.typepad.com/files/jones_gps.pdf.

71. *See* 18 U.S.C. § 2703(d) (2006) (permitting noncontent records from cellular phones to be obtained based on an application establishing specific and articulable facts).

72. 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, *supra* note 70, at 4.

73. *Jones*, 132 S. Ct. at 948.

74. *Id.*

75. *See, e.g.*, United States v. McIver, 186 F.3d 1119, 1126–27 (9th Cir. 1999), *abrogated by Jones*, 132 S. Ct. 945.

76. *Cf.* People v. Weaver, 909 N.E.2d 1195, 1203 (N.Y. 2009) (holding that placement and use of a GPS device on a car is a "search" under the New York State constitution).

77. *Jones*, 132 S. Ct. at 948.

The officers used the GPS device to record the location of Jones's car for twenty-eight days. The battery-powered GPS device could record the location of the car within approximately 50 to 100 feet.[78] 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. The device produced over 2,000 pages of location data over twenty-eight days. The location information helped show that Jones's movements were coordinated with those of his co-conspirators, and that he would rendezvous with his co-conspirators and visit the stash house in Fort Washington, Maryland, where the drugs and cash were later found.[79]

At trial, the prosecution attempted to admit the GPS evidence to show that Jones was involved in the conspiracy. Jones moved to suppress the GPS evidence. Judge Ellen Huvelle agreed with Jones that any evidence indicating that the car was inside Jones's garage had been obtained in violation of the Fourth Amendment.[80] However, 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 broadcasted 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 any 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]

B. *The D.C. Circuit's Opinion in* Maynard

Maynard and Jones appealed their convictions, although only Jones challenged the GPS evidence used to convict him at trial. Jones argued on appeal that *Knotts* was distinguishable because a GPS device was "light

78. *Id.*

79. *See id.* at 948–49.

80. United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006), *aff'd in part, rev'd in part sub nom.* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

81. 460 U.S. 276 (1983).

82. *Knotts*, 460 U.S. at 281–82.

83. *Jones*, 451 F. Supp. 2d at 88.

84. *Jones*, 132 S. Ct. at 948–49.

years away"[85] from a radio beeper. Far from merely enhancing the senses, the GPS device could gather 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 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 Jones's conviction on the ground that use of the GPS device over twenty-eight 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 installing and monitoring a GPS device was one such dragnet-type 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 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 twenty-eight days, *considered as a collective whole*, would be so exposed.

---

85. *See* Brief for Appellants at 54, United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) (No. 08-3030), 2009 WL 3155141.

86. April A. Otterberg, *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 for Appellants, *supra* note 85, at 60 (quoting Otterberg, *supra* note 86, at 696–97).

88. United States v. Maynard, 615 F.3d 544, 568 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

89. *Id.* at 556–58 (citing United States v. Knotts, 460 U.S. 276, 283–84 (1983)).

90. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 508–12 (2007).

91. *Id.*

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

In his view, the monitoring over time 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 Jones's movements 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 were exposed in a constructive sense—that is, exposed even if no one actually observed them—the collective entity of the twenty-eight days of surveillance was not so exposed. This was true because the collective sum of twenty-eight 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 nonsearches packaged 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, *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*.[96] *Reporters Committee* 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.[97] 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."[98]

---

93. *Id.*
94. *Id.* at 560.
95. *Id.* at 562.
96. 489 U.S. 749 (1989).
97. *Reporters Committee*, 489 U.S. at 779–80.
98. *Id.* at 764.

Judge Ginsburg argued that the same mosaic principle should apply in the Fourth Amendment setting. The whole was not merely the sum of its 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.[99]

When considered as a collective whole, the monitoring over twenty-eight days was a Fourth Amendment search because it revealed "an intimate picture of the subject's life that he expects no one to have—short perhaps of his spouse."[100] The D.C. Circuit denied rehearing over several dissents, including one by Judge Kavanaugh that pointed to an alternative rationale: perhaps the installation of the device, rather than its use, constituted the search.[101]

C. *The Supreme Court's Opinions in* Jones

The Supreme Court unanimously agreed that Jones had been the subject of a Fourth Amendment search but divided sharply on why.[102] Writing for a five-justice majority, Justice Scalia followed Judge Kavanaugh's suggestion and held that the installation of the GPS device was a search because it was a trespass on the "effects" of the car.[103] Having resolved the case on trespass grounds, Justice Scalia did not need to reach the mosaic theory adopted in the D.C. Circuit.[104] However, five justices wrote or joined opinions that did touch on the mosaic theory. 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 first opinion to consider is Justice Alito's concurrence in the judgment. Justice Alito wrote for four justices, as his opinion was joined by

---

99. *Maynard*, 615 F.3d at 562.

100. *Id.* at 563.

101. *See* United States v. Jones, 625 F.3d 766, 769–71 (D.C. Cir. 2010) (Kavanaugh, J., dissenting), *denying reh'g en banc to* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

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

103. *Id.* at 951–54.

104. *Id.* at 953–54.

Justices Ginsburg, Breyer, and Kagan.[105] Most of Justice Alito's opinion criticized the majority's trespass rationale.[106] Near the end, however, his opinion turned to how he would have resolved the case under the reasonable expectation of privacy test[107] Justice Alito accepted *United States v. Knotts* but construed it as limited to "relatively short-term monitoring of a person's movements."[108] According to Justice Alito, the long-term monitoring of the car presented a different issue.[109]

Justice Alito applied the reasonable expectation of privacy test by invoking expectations of how law enforcement investigate particular crimes. According to Justice Alito, society has an expectation as to how different offenses 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"[110] monitor the location of the suspect's car in the detailed way GPS monitoring enabled. The same might not be true of an "extraordinary offense[],"[111] Justice Alito suggested. For "extraordinary" crimes, such extensive monitoring might be expected based on "previously available techniques."[112] But because the conspiracy in *Jones* was not, in Justice Alito's view, "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, his opinion 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.[113] 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, which 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 twenty-eight days exceeded societal expectations. Implicitly, the unit of the search was a collective whole over an extended period of time.

The fifth justice to touch on the mosaic theory was Justice Sotomayor. Justice Sotomayor joined the majority opinion and also agreed with Justice Alito that use of a GPS device constituted a search, independent of its installation. Justice Sotomayor reasoned that "the unique attributes of GPS

105. *Id.* at 957–64 (Alito, J., concurring in the judgment).
106. *Id.* at 958–62.
107. *Id.* at 963–64.
108. *Id.* at 964.
109. *Id.*
110. *Id.*
111. *See id.*
112. *Id.*
113. *Id.*

monitoring"[114]—its precision, detail, and efficiency—should guide the constitutional analysis of its use:

> 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 sums from the mosaic theory, not the language 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 opinion focused on surprise. It looked to whether the investigation exceeded society's expectations for how the police would investigate a particular crime.[116] In contrast, Justice Sotomayor's approach looked 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* analyze the collective sum of government action, rather than individual sequential steps, to determine what counts as a Fourth Amendment search.

III. IMPLEMENTING THE MOSAIC THEORY

The possible adoption of the mosaic theory raises challenging new questions for the future of Fourth Amendment law. It is undoubtedly true that combining many pieces of information about suspects can lead the government to learn intimate details about their lives.[118] In the past, however, this was considered good police work rather than cause for alarm. The repeated use of nonsearch techniques has been considered an essential way to create probable cause that justifies searches rather than an unlawful search itself.[119]

---

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

115. *Id.* at 956.

116. *See id.* at 964 (Alito, J., concurring in the judgment).

117. *See id.* 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 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. Enters., Inc., 498 U.S. 292, 297 (1991) ("[T]he Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence

The very different premises of the mosaic theory open a wide range of new questions for courts to answer.

This Section analyzes 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 require the creation of a parallel set of Fourth Amendment rules. For every settled question of law under the sequential approach, courts would need to reanalyze the framework under the mosaic theory. And, for the most part, the mosaic version would be 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 concerns the standard that would govern 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 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.* If courts adopt a mosaic theory, they will need a theory of grouping to explain how conduct should be grouped to assess whether the collective whole crosses the mosaic line. The mosaic theory groups conduct that is not a search and asks if the nonsearches considered together cross the line to become a search. This requires courts to answer a series of grouping questions. Which surveillance methods prompt a mosaic approach? Should courts group across surveillance methods? If so, how? What is the half-life of a mosaic search?

3. *Constitutional Reasonableness.* The next question is how to analyze the reasonableness of mosaic searches. Mosaic searches do not fit an obvious doctrinal box for determining reasonableness. The nature of the mosaic is that each mosaic will be different, potentially requiring different kinds of reasonableness analyses 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 therefore have to create a framework for determining the reasonableness of mosaic searches.

4. *Remedies for Mosaic Violations.* The final question concerns what remedies should apply to unconstitutional mosaic searches. Does the

---

sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists.").

120. EDWIN A. ABBOTT, FLATLAND: A ROMANCE OF MANY DIMENSIONS (5th ed., Harper & Row 1963) (1884).

exclusionary rule apply? If so, does the rule extend over all of the mosaic or only the surveillance that crossed the line to trigger a search? Who has standing to challenge mosaic searches? How should courts apply remedial limitations such as inevitable discovery given that only parts of the mosaic may have been inevitably discovered? 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 doctrine.

A. *Identifying the Standard*

The first challenge raised by the potential adoption of a mosaic theory is selecting the proper standard for aggregation. This question divides into two parts. The first requires identifying the proper reference point for when a mosaic has been created. The second requires choosing which stages of surveillance the mosaic theory regulates: initial data collection, subsequent analysis, or both.

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 theory, Judge Ginsburg offered yet another standard, focusing on whether the government learned more than a stranger could have observed. These approaches are quite different. If courts adopt the mosaic theory, which version should they use?

Choosing among the different versions of the mosaic theory is particularly difficult because each formulation contains major ambiguities. Consider Justice Alito's approach, which focuses 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. Objective standards are used widely within Fourth Amendment law. But most people lack direct experience with police investigations. As a result, they have little basis on which to estimate what is common or uncommon about particular investigations. Even among

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

122. *Id.*

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

124. *Id.* at 964 (Alito, J., concurring in the judgment).

experienced officers, reasonable estimates will diverge. Different agencies investigate different cases in different circumstances in different ways.

Given the public's poor understanding of police practices and the wide variation among those practices, it is unclear what courts are supposed to measure or how they are supposed to measure it.[125] Nor is it clear what kind of deviations from that expectation can trigger the mosaic. Investigations can involve many people using many tools over time. Any reasonably competent defense attorney can find at least some aspect of an 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.

Justice Sotomayor's 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."[126] 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 about a person's "political and religious beliefs, sexual habits, and so on." Courts must then determine whether the public has the reasonable expectations 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 private actors would conduct similar surveillance. What do courts know about the kinds of surveillance practices that businesses, marketers, and private investigators might conduct? How similar is similar enough? Is the relevant standard whether the aggregation of evidence exceeds societal expectations of what one single stranger would see, or what all strangers collectively would see? 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 would regulate. Surveillance regimes often involve several stages: first, the acquisition of information; second, the analysis of that information; and third, the use or disclosure of that information.[127] Fourth Amendment law traditionally has focused only on the first step—the acquisition of information.[128] The

125. I develop this point further *infra* in Section IV.B.2.

126. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

127. Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law* 4–5 (Brookings Inst. The Future of the Constitution Series, 2011), *available at* http://www.brookings.edu/~/media/research/files/papers/2011/4/19%20surveillance%20laws%20kerr/0419_surveillance_law_kerr.pdf.

128. *Id.* at 6, 9–10.

subsequent analysis and use of information has been considered beyond the scope of Fourth Amendment protection.[129]

The mosaic theory could change this. Justice Alito's opinion in *Jones* looked to whether a person reasonably expects others to "secretly monitor *and catalog*"[130] a person's movements. Justice Sotomayor asked "whether people reasonably expect that their movements will be recorded *and aggregated*"[131] in a manner that creates the mosaic. Cataloging and aggregating are verbs that describe subsequent analysis instead of initial collection. These phrases suggest that the mosaic theory requires some step beyond the acquisition stage.

If so, courts will need to determine what kinds of postacquisition conduct are required to create a mosaic. Imagine the government collects a great deal of 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 of the evidence is required to trigger the mosaic, what kind of analysis counts? Does any analysis suffice, or is there some 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.[132] If private parties conduct surveillance, that surveillance cannot constitute a Fourth Amendment search unless the parties acted as agents of the government.[133] The state action requirement raises difficult questions because government agents and private parties can divide surveillance tasks. To see the problem, imagine that a private party collects mosaic data without government involvement. Now imagine that the government obtains a court order compelling the private party to disclose it, or that 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? 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

---

129. 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, 797 (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 (1983) ("[O]nce police are lawfully in a position to observe an item firsthand, its owner's privacy interest in that item is lost.").

130. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) (emphasis added).

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

132. United States v. Jacobsen, 466 U.S. 109, 113–14 (1984).

133. *See id.*

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 on a standard to gauge if a mosaic has been created, the next question is how to solve the grouping problem. The mosaic theory looks at an aggregated set of data acquisitions, and it determines when they trigger a collective search. Applying this approach requires a theory of grouping—a theory of what should be aggregated and how—to assess when that trigger point has been reached. Three kinds 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

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 twenty-eight days. Justice Alito stated that this was "surely"[134] long enough to create a mosaic. But he provided no reason why, and he recognized that "other cases may present more difficult questions."[135] If twenty-eight days is too far, how about fourteen days? Or 3.6 days? Where is the line?

Identifying the length of time 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 for only one hour a day. The device is otherwise dormant. If the police monitor that device over twenty-eight days, does that count as twenty-eight days of monitoring? Or is that only twenty-eight *hours* of monitoring?

Software can be configured to collect data in more complex ways, further complicating the problem. Imagine the GPS device is set to record the location of the car only once a month, precisely at midnight on the first day of each 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 triggers a search or "short-term" surveillance that does not? What if the device records once a day or once a week instead of only once a month?

---

134. *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.").

135. *Id.*

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? Assume, for the sake of argument, that the Supreme Court eventually draws the line for continuous GPS monitoring at seven days. When the monitoring has occurred for seven days, a search has occurred. Now imagine that the police monitor a suspect for five 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 three days. Does this count as eight days of monitoring, such that the mosaic was created and the conduct was a search? Or does this count as five days of monitoring in one year and three 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. 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 for 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 matter independently of police knowledge or if some police knowledge is required.

2. Which Surveillance Methods Count?

The next set of questions considers 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 many that investigators used. The government obtained cell phone location records, installed a public surveillance camera, and watched the suspects in public, all in addition to tapping phones and obtaining text messages.[137] When considering whether 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 transmitted from the suspect's phone to the suspect's service provid-

136. An additional complication is that a group of coconspirators 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 a GPS device installed for different periods of time).

137. *See supra* notes 62–71.

er?[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. If courts adopt the mosaic approach, they will need to answer whether the mosaic theory applies to these techniques.

The next question is whether the mosaic theory only applies to location surveillance. The GPS device in *Jones* broadcast the location of Jones's car, and the collective record of the location of the car over time allowed 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 email address a suspect wrote to and every telephone number a suspect dialed. Investigators might monitor the IP address of every website that a suspect visited. They might obtain a suspect's credit card statements showing purchases the suspect made over many months. If the mosaic theory applies to location monitoring, courts will need to consider whether the same theory extends to other kinds of surveillance.

If the mosaic theory applies to multiple surveillance methods, courts must also consider whether the duration and scale questions raised earlier should be answered in the same way for every method. Different methods of surveillance have different levels of invasiveness. As a result, different methods of surveillance might require different regulation within the mosaic framework. 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 question is whether and how to group across them. In *Maynard/Jones*, the police simultaneously monitored a suspect using cell-site tracking, visual surveillance, and GPS monitoring.[140] If the mosaic theory applies to each surveillance method individually, should courts apply the theory to each surveillance method in isolation? Or should they ask whether the collective of

---

138. *See, e.g.*, United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012) (rejecting the mosaic theory for collection of cell-site data).

139. *See, e.g.*, Mont. State Fund v. Simms, 270 P.3d 64, 69–72 (Mont. 2012) (Nelson, J., specially concurring) (suggesting that the mosaic theory should apply to public camera surveillance).

140. *See supra* notes 62–73.

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?

Because multiple investigations can target the same suspect, courts may need to consider whether the mosaic aggregates across different investigations. Imagine a suspect is under investigation by both federal and state authorities. After the suspect buys a car that has a GPS device installed on it, the state investigators turn on the GPS device. They monitor the suspect for five days and then cease 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 develop a theory of grouping, they must next articulate a framework for analyzing the reasonableness of mosaic searches. Recall that 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 they then determine how much regulation of that step is needed to ensure its use is constitutionally reasonable.[143] For some searches, courts require a warrant based on probable cause.[144] For other searches, they require just probable cause, or reasonable suspicion, or even no suspicion at all?[145] How should this framework apply to mosaic searches? Should mosaic searches require search warrants, and if so, how should such warrants be drafted? If warrants are not required, what level of cause must be established?

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

---

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); United States v. Bailey (*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).

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

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 (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 they 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 space? No court has ever considered the question before *Jones* because public-location surveillance has not 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 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.[156] Courts could apply those precedents

147. *See Carney*, 471 U.S. at 392–94.

148. *Terry*, 392 U.S. at 27.

149. Samson v. California, 547 U.S. 843, 857 (2006).

150. Kentucky v. King, 131 S. Ct. 1849, 1858 (2011).

151. United States v. Jones, 132 S. Ct. 945, 954 (2012).

152. To be sure, in *United States v. Karo*, the Supreme Court did rule that use of a radio beeper to determine the location of property inside a home requires a warrant. 468 U.S. 705, 714 (1984). But the reason was that the beeper disclosed information about the inside of a home, which traditionally requires a warrant. *See id.* at 718–19.

153. *E.g.*, Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches 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.").

154. *E.g.*, State v. Zahn, 812 N.W.2d 490, 499 (S.D. 2012) (suggesting that a warrant is required for mosaic searches because no exception to the warrant requirement applies).

155. *See, e.g.*, *id.* ("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

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 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. Courts will need to consider if the reasonableness of a mosaic search is a "one-size-fits-all" question or if 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 less 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 depends on the context. The question is, *probability of what*? When the Fourth Amendment requires probable cause to arrest, for example, the relevant probable cause is probable cause to believe that a crime has been committed and that the suspect committed it.[158] When the Fourth Amendment requires search warrants, however, the probable cause requirement refers to 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 different kinds of probable cause.

This prompts an intriguing question: if mosaic searches require probable cause, then what kind of probable cause do they require? Must investigators establish probable cause to believe that the location of the suspect is evidence of a crime? Must they establish probable cause to believe that the suspect monitored has committed a crime? Or perhaps some other standard applies?

A recent decision 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 govern-

---

control conduct of law enforcement officers that may significantly intrude upon privacy interests" that "[s]ometimes . . . require warrants" and other times do not (quoting Texas v. Brown, 460 U.S. 730, 739 (1983)) (internal quotation marks omitted)).

157. *See, e.g.*, California v. Carney, 471 U.S. 386, 392–94 (1985).

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

159. *Id.* at 307.

160. *See In re* Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., No. 10-2188-SKG, 2011 WL 3423370 (D. Md. Aug. 3, 2011).

ment's application established probable cause to believe that 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 because the government proved the wrong kind of probable cause. In the magistrate's opinion, the Fourth Amendment requires probable cause that the evidence sought by the warrant was itself evidence of a crime.[161] The Fourth Amendment did not permit the issuance of a warrant because the fugitive's current location was not itself evidence of a crime.[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. 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? The world? The court's jurisdiction? 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 take place or only where the collection occurs? Similar problems arise with the requirement of particularly describing the "thing" to be "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. Given these difficulties, it is unclear how or whether courts can reconcile the mosaic search theory and the particularity requirement.[167]

---

161. *See id.* at *27–30.

162. *Id.* at *30.

163. U.S. CONST. amend. IV.

164. *See supra* Section III.A.2.

165. *Cf.* United States v. Freitas, 800 F.2d 1451, 1455 (9th Cir. 1986) (noting that a warrant rule permitting officers to obtain a warrant to 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*, the Supreme Court suggested that when the police needed to obtain a warrant to use a radio beeper, the place to

D. *Remedies for Mosaic Searches*

The final set of questions concerns the scope of remedies for unconstitutional mosaic searches. Three questions must be answered: first, whether the exclusionary rule should apply to mosaic search violations; second, who has standing to challenge mosaic searches; and third, the proper scope of the fruit of the poisonous tree and inevitable discovery doctrines.

1. Does the Exclusionary Rule Apply?

The first significant question is whether mosaic search violations should trigger the exclusionary rule. Under the exclusionary rule, the government cannot use at trial evidence obtained in violation of the Fourth Amendment. The scope of the exclusionary rule is complex and currently in a state of considerable flux. But the scope of the exclusionary rule for mosaic violations would raise particularly difficult questions.

The first question is whether mosaic violations would be categorically exempt from the exclusionary rule under *Hudson v. Michigan*.[168] In *Hudson*, the Supreme Court held that the suppression remedy is not available for violations of the Fourth Amendment "knock-and-announce" rule.[169] 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.[170] *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,[171] 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.[172]

---

be searched was "the object into which the beeper is to be placed." 468 U.S. 705, 718 (1984). 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* United States v. Jones, 132 S. Ct. 945, 957–58 (2012) (Alito, J., concurring in the judgment).

Case law on the particularity requirement for roving wiretaps provides another reference point that is of only limited value. 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, *e.g.*, United States v. Petti, 973 F.2d 1441, 1445 (9th Cir. 1992), roving wiretaps still state the place to be searched, *e.g.*, *id.* ("Only telephone facilities actually used by an identified speaker may be subjected to surveillance . . . ."). 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.

168. 547 U.S. 586 (2006).

169. *Hudson*, 547 U.S. at 599.

170. Wilson v. Arkansas, 514 U.S. 927, 931–34 (1995).

171. *See Hudson*, 547 U.S. at 594–95, 598.

172. *See id.* at 598–99.

If courts recognize mosaic searches, they will need to consider whether mosaic violations are exempt from the exclusionary rule under *Hudson*. On one hand, courts might plausibly analogize mosaic search violations to knock-and-announce violations. Both involve murky standards 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. 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.[173] 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.[174] Although the cases are not a model of clarity, they seem to indicate that the violation must be intentional, reckless, or grossly negligent to justify suppression.[175] Otherwise, the violation is one in "good faith" and no exclusionary rule applies.[176] 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 might not apply.

Privacy statutes may also limit the scope of the exclusionary rule. Under *Illinois v. Krull*,[177] 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.[178] To the extent the scope of the mosaic theory remains unclear, officers who follow statutes regulating GPS surveillance are likely to avoid suppression even if courts

---

173. *See id.* at 603 (Kennedy, J., concurring in part and concurring in the judgment).

174. *See, e.g.*, Davis v. United States, 131 S. Ct. 2419, 2427–28 (2011).

175. *See id.* (citing Herring v. United States, 555 U.S. 135, 137 (2009)).

176. *See id.*

177. 480 U.S. 340, 355 (1987).

178. For example, Minnesota Statute sections 626A.35 through 626A.37 require the government to obtain a court order to install a mobile tracking device, and authorize surveillance for up to sixty 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 (West 2009). 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).

take a more restrictive view of the GPS surveillance than do the relevant statutes.[179]

2. Standing to Challenge Mosaic Searches

If the exclusionary rule generally applies to mosaic search violations, courts will need to determine its scope. The first challenge is identifying who has standing to challenge a mosaic search. Fourth Amendment rights are personal, and individuals can invoke a remedy only if their own rights have been violated.[180] The Fourth Amendment standing inquiry arises as an application of the reasonable expectation of privacy test. Every defendant must establish that his or her own reasonable expectation of privacy was violated to merit a ruling suppressing the evidence.[181]

Standing raises difficult challenges for the mosaic theory because conduct that creates a mosaic may involve monitoring different people at different times to different degrees. Consider the facts of a recent district court case, *United States v. Luna-Santillanes*.[182] Three conspirators ran a heroin trafficking enterprise and shared three cars. Different drivers drove the three different cars at different times. Investigators installed GPS devices on all three cars and used the GPS devices to track the movements of the three defendants.[183] The first car was monitored for two months; the second car was monitored for what the court called "a few" days; and the third car was monitored for only two days.[184]

Assuming that the collective monitoring of the three cars constituted a search, who has standing to challenge it? Do all three defendants have standing because their location was monitored as part of a broader mosaic? Or must the standing inquiry look to each individual and consider whether the monitoring of that particular defendant was enough to constitute its own mosaic? Or perhaps the standing inquiry should operate on a car-by-car basis, limiting standing to primary drivers or passengers of particular cars?[185] If the exclusionary rule applies to mosaic searches, courts will need to develop answers to these questions.

---

179. 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*, 131 S. Ct. at 2423–24 (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 the discrete-steps approach factors in reliance on binding precedent. *See id.*

180. Minnesota v. Carter, 525 U.S. 83, 99 (1998) (Kennedy, J., concurring) ("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.").

181. *See* Rakas v. Illinois, 439 U.S. 128 (1978).

182. No. 11-20492, 2012 WL 1019601, at *1 (E.D. Mich. Mar. 26, 2012).

183. *Luna-Santillanes*, 2012 WL 1019601, at *1–4.

184. *Id.* at *7 n.4.

185. *Cf.* United States v. Hanna, No. 11-20678-CR, 2012 WL 279435, at *4 (S.D. Fla. Jan. 30, 2012) ("For purposes of this analysis under *Jones*, one must have an expectation of privacy as to the particular vehicle tracked, either from an ownership or possessory interest.").

3. Fruit of the Poisonous Tree and Inevitable Discovery

Assuming the exclusionary rule applies and defendants have standing, the next question is whether the unconstitutional conduct justifies suppression because it acts as both the but-for and proximate cause of the discovery of the relevant evidence. In the context of the exclusionary rule, these questions arise under the rubric of the "fruit of the poisonous tree" and "inevitable discovery" doctrines.[186] These doctrines raise puzzling questions for mosaic violations because it is difficult to identify the unconstitutional mosaic act. Is the aggregated mosaic a single unconstitutional act, or is the unconstitutional act only the surveillance that occurred after the monitoring became a search?

Consider whether the exclusionary rule applies to the entire mosaic or only some part of it. To simplify matters, let's use the prior 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 search line was crossed? Further, imagine the police learn on day two of the ongoing surveillance that the suspect committed a crime. Should the evidence from day two be suppressed because it was part of the mosaic triggered after seven days, even though the collection of that evidence was not a search when it occurred? Or is the evidence from day two 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 moment rather than to develop a picture of their lives over time. Consider a recent case involving a GPS device attached to a car used to transport heroin.[187] Investigators used 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.[188] Assuming the GPS device was used long enough to cross the threshold of a search, should the heroin be suppressed as a fruit of the poisonous mosaic search? Or does the exclusionary rule not apply because the stop was the product of a short-term use of the GPS device rather than a broader mosaic? 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*[189] do not establish the theory as a matter of law. The majority opinion in *Jones*

186. *See supra* notes 51–53 and accompanying text.

187. *Luna-Santillanes*, 2012 WL 1019601, at *1–2.

188. *See id.*

189. 132 S. Ct. 945 (2012).

did not adopt the mosaic approach, and it only touched on the method in passing to express skepticism.[190] Sequential precedents remain binding on lower courts even if five justices seem prepared to take a new path. For now, the sequential approach remains the basic standard of Fourth Amendment doctrine. 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 adopt 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 Part 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,"[191] 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 halfway measure. Under the sequential approach, courts traditionally have two options when deciding how to regulate police conduct. They can decide that particular conduct is *never* a Fourth Amendment search but that legislatures can regulate the conduct by enacting statutory protections, or they can say that the 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 the principles that should govern this middle ground is extremely difficult, however, such that the challenges of the method outweigh its possible benefits. As Part III explained, 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. Even proponents of the mosaic approach appear not to have answers for how it should apply.[192] 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. If courts must expand Fourth Amendment privacy protections in response to new technologies, they can conclude that the disputed conduct is always a search under a sequential analysis. The model for this approach is the most famous Fourth Amendment decision: *Katz v. United*

---

190. *See Jones*, 132 S. Ct. 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?").

191. *See* Kerr, *supra* note 16.

192. *See infra* notes 204–208 and accompanying text.

States.[193] *Katz* shows that rejecting the mosaic theory does not mean rejecting broad Fourth Amendment protection. It only means rejecting the awkward halfway measure of the mosaic theory.

A. *The Mosaic Theory as Equilibrium-Adjustment*

In a recent article,[194] 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 the government's 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 to 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 downward slopes.[195]

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" was necessarily limited, while computers changed massive-scale monitoring from something "impractical" to something "relatively easy and cheap."[196] Such new powers "may 'alter the relationship between citizen and government,' "[197] Justice Sotomayor worried, resulting in "a tool so amenable to misuse"[198] that Fourth Amendment doctrine needed to respond.

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, their use remains outside the scope of Fourth Amendment protection. But if the government fully exploits the new powers the new tools provide, the scope of surveillance upsets the earlier balance and the mosaic theory subjects the government's conduct to Fourth Amendment oversight.

---

193. 389 U.S. 347 (1967).

194. *See* Kerr, *supra* note 16.

195. *See id.* at 487–90 (explaining the process of equilibrium-adjustment).

196. *See* United States v. Jones, 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring in the judgment).

197. *Id.* at 956 (Sotomayor, J., concurring) (quoting United States v. Cuevas–Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *vacated*, 132 S. Ct. 1534 (2012) (mem.)).

198. *Id.* (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)) (internal quotation marks omitted).

B. *The Case Against the Mosaic Theory*

The critical question is whether the mosaic theory offers a desirable approach to 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 repudiated for three reasons. First, the theory raises so many novel and puzzling new questions that it would be 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 statutory protections that better regulate surveillance practices outside of the sequential approach.

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—in effect, a mosaic parallel to the sequential precedents that exist today. The problem is not only the number of questions but also 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.

Murky standards are not unknown in Fourth Amendment law, of course. But the murkiness of the mosaic theory is unprecedented. I find it particularly telling that not even the proponents of the mosaic theory have proposed answers for how the theory should apply. For example, in one recent article, a group of scholars who endorsed the mosaic approach dismissed the conceptual difficulties of its implementation on the ground that answering such puzzles "is why we have judges."[199] A pro-mosaic amicus brief in *Jones* signed by several prominent legal academics was similarly nonresponsive.[200] The brief brushed off the difficulties with implementing the mosaic theory by stating that judges encounter vague standards elsewhere in Fourth Amendment law and they can implement the mosaic theory by "consider[ing] the same criteria applied to other surveillance situations."[201]

I appreciate such confidence in judicial abilities. But surely there is a stark difference between applying vague standards and implementing a the-

---

199. *See* Smith et al., *supra* note 15, at 201.

200. *See* Brief of *Amici Curiae*, Yale Law School Information Society Project Scholars and Other Experts in the Law of Privacy and Technology in Support of the Respondent at 25–27, *Jones*, 132 S. Ct. 945 (No. 10-1259), 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. *Id.* at 1–3.

201. *Id.* at 27.

ory so mysterious that Fourth Amendment experts decline to express an opinion on how to apply it. Judges are smart people, but they are not like Moses bringing the tablets down from Mount Sinai. If the questions raised by the mosaic theory can be answered, proponents of the theory should answer them. Expressions of confidence that answers can be found do not substitute for the answers themselves.[202]

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 typically occurs at a more snail-like pace. As a result, the constantly evolving nature of surveillance practices can lead new questions to arise faster than courts might 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 be unknown. Like Lucy and Ethel trying to package candy on the ever-faster conveyor belt,[203] 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 location-tracking technologies was the primitive radio beeper seen in *Knotts*. But radio beepers are obsolete. 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. The 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 eventually may devise answers to the many questions discussed in Part III. But by the time they do, the technology is likely to be obsolete.

---

202. The closest any scholar has come to answering the questions raised by the mosaic theory is Christopher Slobogin, who recently proposed a model statute to implement the mosaic theory. *See* Christopher Slobogin, *Making the Most of* Jones v. United States *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y (forthcoming 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2098002. Professor Slobogin proposes a complex framework distinguishing among "target public searches," "targeted data search of data held by an institutional third party," and "general public and data searches." He would require different standards to conduct different kinds of surveillance for different times, such as twenty minutes or forty-eight hours. *See id.* at 17–22. Importantly, even Professor Slobogin declines to say how the mosaic theory applies. His proposal is statutory rather than constitutional. Further, Professor Slobogin's statutory proposal is similar to arguments he advanced in a recent book on the Fourth Amendment published well before *Jones*. *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007)). I reviewed Professor Slobogin's book in 2009, and my critique of his approach then largely responds to his current proposal. *See* Orin S. Kerr, Review, *Do We Need a New Fourth Amendment?*, 107 MICH. L. REV. 951 (2009).

203. *See I Love Lucy: Job Switching* (CBS television broadcast Sept. 15, 1952).

2. Probabilistic Approaches to the "Reasonable Expectation of Privacy" Test Are Ill Suited to Regulate Technological Surveillance

The second problem with the mosaic theory is that most formulations 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 used several different inquiries to determine what makes an expectation of privacy constitutionally reasonable.[204] In some cases, the Court has looked to what a reasonable person would perceive as likely;[205] in other cases, the Court has looked to whether the particular kind of information obtained is worthy of protection;[206] in some cases, the Court has looked to whether the government violated some legal norm such as a property right in obtaining the information;[207] and in other cases, the Court has simply considered whether the conduct should be regulated by the Fourth Amendment as a matter of policy.[208] 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.[209]

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,[210] as it rests on a notion of the probability of privacy protection. The more likely it is that a person will maintain their privacy, the more likely it is that government conduct defeating that expectation counts as a search. Under this model, the Fourth Amendment guards against surprises. The paradigmatic example is *Bond v. United States*,[211] which involved government agents physically manipulating a bus passenger's duffel bag to identify a wrapped brick of drugs inside it. Manipulating the bag violated a reasonable expectation of privacy because a bus passenger expects other passengers to handle his bag but not to "feel the bag in an exploratory manner."[212] Both Judge Ginsburg and Justice Alito authored mosaic opinions that rely on such probabilistic reasoning.[213] 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 grounds that a rea-

---

204. *See* Kerr, *supra* note 90.
205. *See id.* at 508–12.
206. *See id.* at 512–15.
207. *See id.* at 516–19.
208. *See id.* at 519–22.
209. *See id.* at 543–48.
210. *See id.* at 508–12.
211. 529 U.S. 334 (2000).
212. *Bond*, 529 U.S. at 339.
213. *See supra* Section II.B.

sonable person would not expect the police to obtain so much information.[214]

The probabilistic approach is a poor choice to regulate technological surveillance, however. The problem is a practical one. 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 firsthand. In contrast, estimating the frequency of technological surveillance practices is essentially impossible for most people (including most judges). Surveillance practices tend to be hidden, and few understand the relevant technologies. Some people will guess that privacy invasions are common. Others will guess that they are rare. But exceedingly few will know the truth, which makes probabilistic beliefs a poor basis for Fourth Amendment protection.

Consider the so-called "CSI effect,"[215] by which jurors in routine criminal cases expect prosecutors to introduce evidence collected using high-tech investigatory tools like those 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 hardworking officers with high-tech tools could cut back Fourth Amendment protection by suggesting that very invasive investigations are commonplace. On the other hand, a new show featuring lazy or incompetent officers might expand Fourth Amendment protection by making particularly thorough investigations exceed societal expectations. It is hard to see why such poorly informed beliefs should shape Fourth Amendment protections.

Nor does Supreme Court doctrine require such a result. To the contrary, the Supreme Court has generally avoided applying the probabilistic model to government surveillance practices.[216] The Court has relied instead on other models that provide more stable ways to regulate government surveillance practices.[217] 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.

---

214. *See supra* Section II.C.

215. *See* Simon A. Cole & Rachel Dioso-Villa, *Investigating the 'CSI Effect' Effect: Media and Litigation Crisis in Criminal Law*, 61 STAN. L. REV. 1335, 1336–37 (2009).

216. *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.").

217. *See 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[218]—and as Justice Alito suggested in his concurring opinion in *Jones*[219]—Congress has significant institutional advantages over the courts in trying to regulate privacy in new technologies. Congress can act quickly, hold hearings, and consider expert opinion.[220] Congress can draw arbitrary lines that don't fit easily within constitutional doctrine.[221] And if Congress errs or facts change, Congress can amend its prior handiwork relatively easily.[222] Congress can also regulate using sunset provisions that force the legislature to revisit the question in light of intervening experience.[223] 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.[224] 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 of 1978,[225] passed in response to *United States v. Miller*;[226] the Pen Register Statute,[227] passed in response to *Smith v. Maryland*;[228] and the Privacy Protection Act of 1980,[229] passed in response to *Zurcher v. Stanford Daily*.[230] In all three instances, Congress responded to a Fourth Amendment ruling allowing a controversial investigatory practice

---

218. *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).

219. *See Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment) (citing Kerr, *supra* note 90, at 805–06).

220. Kerr, *supra* note 90, at 870, 881–82.

221. *See id.* at 871–72.

222. *See id.*

223. *See id.* at 873.

224. *Cf. id.* at 855–57.

225. Pub. L. No. 95-630, tit. XI, 92 Stat. 3641, 3697–710 (codified at 12 U.S.C. §§ 3401–3422 (2006)).

226. 425 U.S. 435 (1976).

227. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, sec. 301(a), 100 Stat. 1848, 1868–72 (codified as amended at 18 U.S.C. §§ 3121–3127 (2006 & Supp. IV 2010)).

228. 442 U.S. 735 (1979).

229. Pub. L. No. 96-440, 94 Stat. 1879 (codified as amended at 42 U.S.C. §§ 2000aa, 2000aa-5 to 2000aa-7, 2000aa-11 (2006)).

230. 436 U.S. 547 (1978).

by creating statutory protections.[231] 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.[232]

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 where no statutory protection exists, such that enactment of statutory protections disables the mosaic theory.[233] If so, the mosaic theory could encourage statutory protections rather than discourage them. But this possibility raises its own 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

---

231. *See, e.g.*, H.R. REP. NO. 95-1383, at 34 (1978), *reprinted in* 1978 U.S.C.C.A.N. 9273, 9306 (discussing bills to create statutory right to privacy in financial records in response to *United States v. Miller*, 425 U.S. 435).

232. This is just a prediction, of course, 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. (2011), and Senator Wyden introduced the Geolocational Privacy and Surveillance Act, S. 1212, 112th Cong. (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.

233. It is important to avoid reading too much into the penumbras of Supreme Court opinions. Such overreading can purport to find signals that no justice intended. 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." United States v. Jones, 132 S. Ct. 945, 964 (2012) (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, 342, 349–50 (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." *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring). This seems to suggest that oversight from a coordinate branch such as Congress might lead her to reach a different interpretation of the Fourth Amendment.

laws.[234] A few state supreme courts had regulated GPS monitoring under state constitutions.[235] 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 would be entirely procedural: legislatures would only 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.[236]

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, judges can engage in equilibrium-adjustment within the context of a binary choice. Judges can rule that government conduct is not a search and thereby leave it to statutory regulation, or they can decide it is 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 contexts, and it then flips the switch and calls the government action a search when grouped together in some broader or longer-term contexts. Consider the use of GPS devices in *Maynard/Jones*. In *United States v. Knotts*, the Court had held that use of a location device to monitor the location of a car on public thoroughfares was never a search.[237] In his mosaic concurrence in *Jones*, Justice Alito reaffirmed the *Knotts* precedent but limited it to "relatively short-term monitoring of a person's

234. *See, e.g.*, FLA. STAT. § 934.06 (2011); MINN. STAT. ANN. § 626A.37 (West 2009).

235. *See, e.g.*, State v. Jackson, 76 P.3d 217, 263–64 (Wash. 2003).

236. *See* Orin S. Kerr, *Congress, the Courts, and New Technologies: A Response To Professor Solove*, 74 FORDHAM L. REV. 779, 787–90 (2005).

237. 460 U.S. 276, 281–82 (1983).

movements on public streets."[238] 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 this middle ground, it would allow judges to continue to engage in equilibrium-adjustment by expanding what constitutes a search. The proper model is *Katz v. United States*,[239] 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.[240]

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 and 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. It aims to restore the balance of Fourth Amendment protection by disabling the new powers created by computerization of surveillance tools. But despite these good intentions, 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. The concurring

238. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment).

239. 389 U.S. 347 (1967).

240. *Katz*, 389 U.S. at 353, 359.

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.

STATUTORY INSTRUMENTS

2002 No. 1438

NATIONAL HEALTH SERVICE, ENGLAND AND WALES

The Health Service (Control of Patient Information) Regulations 2002

Made - - - - *23rd May 2002*

Coming into force *1st June 2002*

Whereas a draft of the following Regulations was laid before Parliament in accordance with section 64(3) of the Health and Social Care Act 2001**(a)** and was approved by resolution of each House of Parliament:

Now, therefore, the Secretary of State for Health, in exercise of the powers conferred on him by sections 60(1) and 64(6), (7) and (8) of the Health and Social Care Act 2001 and all other powers enabling him in that behalf, having consulted such bodies as appear to him to represent the interests of those likely to be affected by the Regulations in accordance with section 60(7) of that Act and having sought and had regard to the views of the Patient Information Advisory Group**(b)** on the proposed Regulations in accordance with section 61(2) of that Act, hereby makes the following Regulations—

Citation, commencement, interpretation and extent

1.—(1) These Regulations may be cited as the Health Service (Control of Patient Information) Regulations 2002 and shall come into force on 1st June 2002.

(2) In these Regulations—

"the Act" means the Health and Social Care Act 2001,

"public authority" has the same meaning as in section 3(1) of the Freedom of Information Act 2000**(c)**;

"public health laboratory service" means the microbiological service provided by the Public Health Laboratory Service Board under section 5(2)(c) and (4) of the National Health Service Act 1977**(d)**;

"research ethics committee" means a local research ethics committee established or recognised by a health authority within its area or a multi-centre research ethics committee which is recognised by Secretary of State in respect of research carried out within five or more health authority areas or any other research ethics committee recognised by the Secretary of State.

(3) Any notice given under these Regulations shall be—

(a) 2001 c.15.
(b) *See* S.I. 2001/2836.
(c) 2000 c.36.
(d) 1977 c.49; subsections (2)(c) and (4) of section 5 were amended by the Public Health Laboratory Service Act 1979 (c.23), section 1.

(a) in writing; or

(b) transmitted by electronic means in a legible form which is capable of being used for subsequent reference.

(4) Any reference in these Regulations to a numbered regulation is a reference to the regulation which bears that number in these Regulations and any reference to a numbered paragraph in a regulation is a reference to the paragraph which bears that number in that regulation.

(5) These Regulations extend to England and Wales only.

Medical purposes related to the diagnosis or treatment of neoplasia

2.—(1) Subject to paragraphs (2) and (3) and regulation 7, confidential patient information relating to patients referred for the diagnosis or treatment of neoplasia may be processed for medical purposes approved by the Secretary of State which comprise or include—

(a) the surveillance and analysis of health and disease;

(b) the monitoring and audit of health and health related care provision and outcomes where such provision has been made;

(c) the planning and administration of the provision made for health and health related care;

(d) medical research approved by research ethics committees;

(e) the provision of information about individuals who have suffered from a particular disease or condition where—

(i) that information supports an analysis of the risk of developing that disease or condition; and

(ii) it is required for the counseling and support of a person who is concerned about the risk of developing that disease or condition.

(2) For the purposes of this regulation, "processing" includes (in addition to the use, disclosure or obtaining of information) any operations, or set of operations, which are undertaken in order to establish or maintain databases for the purposes set out in paragraph (1), including—

(a) the recording and holding of information;

(b) the retrieval, alignment and combination of information;

(c) the organisation, adaption or alteration of information;

(d) the blocking, erasure and destruction of information.

(3) The processing of confidential patient information for the purposes specified in paragraph (1) may be undertaken by bodies or persons who (either individually or as members of a class) are—

(a) approved by the Secretary of State, and

(b) authorized by the person who lawfully holds the information.

(4) Where the Secretary of State considers that it is necessary in the public interest that confidential patient information is processed for a purpose specified in paragraph (1), he may give notice to any body or person who is approved and authorized under paragraph (3) to require that body or person to process that information for that purpose and any such notice may require that the information is processed forthwith or within such period as is specified in the notice.

(5) Where confidential information is processed under this regulation, the bodies and persons approved under paragraph (3) shall make available to the Secretary of State such information as he may require to assist him in the investigation and audit of that processing and in his annual consideration of the provisions of these Regulations which is required by section 60(4) of the Act.

Communicable disease and other risks to public health

3.—(1) Subject to paragraphs (2) and (3) and regulation 7, confidential patient information may be processed with a view to—

(a) diagnosing communicable diseases and other risks to public health;

(b) recognising trends in such diseases and risks;

(c) controlling and preventing the spread of such diseases and risks;

(d) monitoring and managing—

(i) outbreaks of communicable disease;

(ii) incidents of exposure to communicable disease;

(iii) the delivery, efficacy and safety of immunisation programmes;

(iv) adverse reactions to vaccines and medicines;

(v) risks of infection acquired from food or the environment (including water supplies);

(vi) the giving of information to persons about the diagnosis of communicable disease and risks of acquiring such disease.

(2) For the purposes of this regulation, "processing" includes any operations, or set of operations set out in regulation 2(2) which are undertaken for the purposes set out in paragraph (1).

(3) The processing of confidential patient information for the purposes specified in paragraph (1) may be undertaken by—

(a) the Public Health Laboratory Service;

(b) persons employed or engaged for the purposes of the health service;

(c) other persons employed or engaged by a Government Department or other public authority in communicable disease surveillance.

(4) Where the Secretary of State considers that it is necessary to process confidential patient information for a purpose specified in paragraph (1), he may give notice to any body or person specified in paragraph (3) to require that body or person to process that information for that purpose and any such notice may require that the information is processed forthwith or within such period as is specified in the notice.

(5) Where confidential information is processed under this regulation, the bodies and persons specified in paragraph (3) shall make available to the Secretary of State such information as he may require to assist him in the investigation and audit of that processing and in his annual consideration of the provisions of these Regulations which is required by section 60(4) of the Act.

Modifying the obligation of confidence

4. Anything done by a person that is necessary for the purpose of processing confidential patient information in accordance with these Regulations shall be taken to be lawfully done despite any obligation of confidence owed by that person in respect of it.

General

5. Subject to regulation 7, confidential patient information may be processed for medical purposes in the circumstances set out in the Schedule to these Regulations provided that the processing has been approved—

(a) in the case of medical research, by both the Secretary of State and a research ethics committee, and

(b) in any other case, by the Secretary of State.

Registration

6.—(1) Where an approval granted by the Secretary of State under regulation 5 permits the transfer of confidential patient information between bodies or persons who may determine the

purposes for which, and the manner in which, the information may be processed, he shall record in a register the name and address of the bodies or persons to whom that information may be transferred together with the particulars specified in paragraph (2).

(2) The following particulars are specified for inclusion in each entry in the register—

(a) a description of the confidential patient information to which the approval relates;

(b) the medical purposes for which the information may be processed;

(c) the provisions in the Schedule to these Regulations under which the information may be processed; and

(d) such other particulars as the Secretary of State may consider appropriate to enter in the register.

(3) The Secretary of State shall retain the particulars of each entry in the register for so long as confidential patient information may be processed under the approval to which the entry relates and for not less than 12 months after the termination of that approval.

(4) The Secretary of State shall, in such manner and to the extent to which he considers it appropriate, publish entries in the register.

Restrictions and exclusions

7.—(1) Where a person is in possession of confidential patient information under these Regulations, he shall not process that information more than is necessary to achieve the purposes for which he is permitted to process that information under these Regulations and, in particular, he shall—

(a) so far as it is practical to do so, remove from the information any particulars which identify the person to whom it relates which are not required for the purposes for which it is, or is to be, processed;

(b) not allow any person access to that information other than a person who, by virtue of his contract of employment or otherwise, is involved in processing the information for one or more of those purposes and is aware of the purpose or purposes for which the information may be processed;

(c) ensure that appropriate technical and organisational measures are taken to prevent unauthorised processing of that information;

(d) review at intervals not exceeding 12 months the need to process confidential patient information and the extent to which it is practicable to reduce the confidential patient information which is being processed;

(e) on request by any person or body, make available information on the steps taken to comply with these Regulations.

(2) No person shall process confidential patient information under these Regulations unless he is a health professional or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(3) For the purposes of paragraph (2) "health professional" has the same meaning as in section 69(1) of the Data Protection Act 1998**(a)**.

Enforcement Procedure

8.—(1) Any person who does not comply with a requirement imposed on him under regulation 2(4) or (5), 3(4) or (5) or 7 may be subject to a civil penalty of not exceeding £5000.

(2) The Secretary of State may determine whether any person has not complied with such a requirement and he may assess whether it is appropriate to impose the maximum civil penalty, a lesser penalty or no penalty having regard to the seriousness of any non-compliance, the circumstances of any person who has not complied and the need to ensure the compliance in respect of any such future requirements.

(a) 1998 c.29.

(3) Any penalty payable under this regulation shall be recoverable by the Secretary of State as a civil debt.

Signed by authority of the Secretary of State for Health

Hazel Blears
Parliamentary Under Secretary of State,
Department of Health

23rd May 2002

THE SCHEDULE

Regulations 5 and 6(2)(c)

General Provisions

Circumstances in which confidential patient information may be processed for medical purposes under regulation 5 and particulars for registration under regulation 6.

1. The processing of confidential patient information for medical purposes with a view to making the patient in question less readily identifiable from that information.

2. The processing of confidential patient information that relates to the present or past geographical locations of patients (including where necessary information from which patients may be identified) which is required for medical research into the locations at which disease or other medical conditions may occur.

3. The processing of confidential patient information to enable a lawful holder of that information to identify and contact patients for the purpose of obtaining consent—

(a) to participate in medical research;

(b) to use the information for medical purposes, or

(c) to allow the use of tissue or other samples for medical purposes.

4. The processing of confidential patient information for medical purposes from more than one source with a view to—

(a) linking information from more than one of those sources;

(b) validating the quality or completeness of—

(i) confidential patient information, or

(ii) data derived from such information;

(c) avoiding the impairment of the quality of data derived from confidential patient information by incorrect linkage or the unintentional inclusion of the same information more than once.

5. The audit, monitoring and analysing of the provision made by the health service for patient care and treatment.

6. The granting of access to confidential patient information in one or more of the above circumstances.

EXPLANATORY NOTE

(This note is not part of the Regulations)

These Regulations make provision for the processing of patient information, including confidential patient information.

Regulation 1 contains definitions of the terms used in the Regulation and provides that the Regulations apply to England and Wales only.

Regulation 2 makes provision relating to the processing of confidential patient information in connection with the construction and maintenance of databases by bodies (known as "cancer registries") which undertake the surveillance of health and disease of patients referred for the diagnosis or treatment of neoplasia. Regulation 2(4) provides powers under which the Secretary of State may require certain persons to process information for those purposes. Regulation 2(5) makes provision for information on the operation of these Regulations to be passed to the Secretary of State.

Regulation 3 makes provision for the processing of confidential patient information for the recognition, control and prevention of communicable disease and other risks to public health. Regulation 3(4) provides powers under which the Secretary of State may require certain persons who perform health service or other public functions to process information where, for example, there is a need to assess whether there is a significant risk to public health. Regulation 3(5) makes provision for information on the operation of these Regulations to be passed to the Secretary of State.

Regulation 4 provides that information may be processed in accordance with these Regulations notwithstanding any common law obligation of confidence.

Regulation 5 and the Schedule to these Regulations makes general provision in relation to the processing of patient information. Such processing is restricted to that approved by the Secretary of State and, in the case of processing for research purposes, the relevant ethics committee.

Regulation 6 requires the Secretary of State to record and make public particulars relating to approvals which permit the transfer of confidential patient information.

Regulation 7 restricts the processing of information under the Regulations, for example by requiring the removal of particulars by which the persons to whom information relates can be identified if that is practical (regulation 7(1)(a)).

Regulation 8 provides for enforcement by civil penalty of the requirements imposed under regulations 2(4) or (5), 3(4) or (5) or 7.

The Schedule to these Regulations sets out the circumstances in which confidential patient information may be processed for medical purposes under regulation 5. The provisions relate, for example, to the processing of confidential patient information in order to identify who should be invited to participate in medical research (paragraph 3) or to enable the auditing, monitoring and analysing the provision made by the health service (paragraph 5).

A Regulatory Impact Assessment has not been prepared for these Regulations. In general the Regulations enable the flow of information and impose no obligations. Where obligations are imposed, they are imposed primarily on those performing functions for public authorities and so any burden imposed on business is considered negligible.