Notre Dame Law Review

Volume 86 | Issue 4 Article 7

7-1-2011

The Mosaic Theory and Fourth Amendment Law

Benjamin M. Ostrander

THE "MOSAIC THEORY" AND FOURTH AMENDMENT LAW

*Benjamin M. Ostrander**

INTRODUCTION

In 2004, an FBI-Metropolitan Police Department Safe Streets Task Force began investigating Antoine Jones, owner of the D.C. nightclub "Levels" and suspected drug kingpin, for narcotics violations.[1] Mr. Jones allegedly ran a drug ring that consisted of at least nine other defendants and spanned from 2003 to 2005, involving hundreds of kilograms of cocaine shipped from Mexico.[2] During the investigation, law enforcement agents used a number of investigative techniques, one being Global Positioning System (GPS) surveillance.[3] The agents secretly planted a GPS device on the undercarriage of a Jeep exclusively driven by Mr. Jones, and for nearly one month the device continuously tracked his movements.[4] At the conclusion of the investigation, the Task Force obtained warrants and seized a large quantity of contraband from the homes of several of the defendants.[5] They also searched an alleged "stash house," and seized ninety-seven kilograms of cocaine, three kilograms of crack cocaine, and more than $800,000[6]—making it the largest cocaine seizure in D.C. history.[7] The digital location pattern that resulted from the month-long tracking of Jones—including his visits to the "stash house"—was used as

* Candidate for Juris Doctor, Notre Dame Law School, 2012; B.A., History, Political Science, University of Iowa, 2009.

1 *See* United States v. Maynard, 615 F.3d 544, 549 (D.C. Cir. 2010); Henri E. Cauvin, *Cash and Cocaine, but No Conviction: Jurors, Lawyers Reflect on Where Case Prosecuting District's Largest Drug Seizure Faltered*, Wash. Post, Mar. 5, 2007, at B08.

2 Jim McElhatton, *GPS Use Voids Conviction: Court Overturns D.C. Man's Drug Sentence*, WASH. TIMES, Aug. 9, 2010, at A2.

3 *See* United States v. Jones, 451 F. Supp. 2d 71, 74 (D.D.C. 2006), *aff'd in part, rev'd in part sub nom. Maynard*, 615 F.3d 544.

4 *See Maynard*, 615 F.3d at 555 & n.*.

5 *See Jones*, 451 F. Supp. 2d at 74.

6 *See id.*

7 *See* McElhatton, *supra* note 2.

evidence implicating his involvement in the cocaine trafficking.[8] Mr. Jones was eventually convicted of conspiracy to distribute and to possess with intent to distribute five or more kilograms of cocaine and fifty grams or more of cocaine base.[9] On appeal, however, the District of Columbia Circuit Court of Appeals overturned Jones's conviction.[10] Relying on a novel and potentially revolutionizing theory[11] in Fourth Amendment law—the "mosaic theory"—the D.C. Circuit held that prolonged GPS tracking constituted a "search" within the meaning of the Fourth Amendment.[12] The "mosaic theory," often used in the national security context,[13] holds that individual law enforcement

8 *See Maynard*, 615 F.3d at 562 n.*.

9 *See id.* at 548.

10 *See id.* at 568.

11 *See* Orin Kerr, *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, The 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 (calling *Maynard* and its use of the "new 'mosaic' theory" a "potentially revolutionary Fourth Amendment decision"). *But see* Julian Sanchez, *GPS Tracking and a 'Mosaic Theory' of Government Searches*, CATO INST. (Aug. 11, 2010, 9:22 PM), http://www.cato-at-liberty.org/gps-tracking-and-a-mosaic-theory-of-government-searches (questioning the novelty of the "mosaic theory" in Fourth Amendment law).

12 *See Maynard*, 615 F.3d at 555–63. The government's petition for rehearing en banc was denied by a five-four vote. *See* United States v. Jones, 625 F.3d 766 (D.C. Cir. 2010).

13 The "mosaic theory" was first expounded in a case regarding a government action to enjoin a former CIA employee from publishing an exposé of the agency. *See* United States v. Marchetti, 466 F.2d 1309, 1318 (4th Cir. 1972). Although the court enjoined the publishing of the exposé on the constitutional executive right to secrecy and a secrecy agreement the former agent had signed, the court gave a prudential justification:

> The significance of one item of information may frequently depend upon knowledge of many other items of information. What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context. The courts, of course, are ill-equipped to become sufficiently steeped in foreign intelligence matters to serve effectively in the review of secrecy classifications in that area.

Id. at 1318. Since *Marchetti*, the "mosaic theory" has been a staple in national security law. In his systematic analysis of the "mosaic theory" in Freedom of Information Act law, David E. Pozen describes the theory:

> The "mosaic theory" describes a basic precept of intelligence gathering: Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information. Combining the items illuminates their interrelationships and breeds analytic synergies, so that the resulting mosaic of information is worth more than the sum of its parts. In the context of national

actions that are not searches become a search when aggregated, as the whole reveals more than the individual acts it comprises.[14] Thus, in the context of electronic tracking, this theory contends that although the tracking of each individual movement is not a search, when aggregated, the resulting location pattern becomes a search as it reveals more than the individual movements it comprises.[15]

This Note suggests that despite the intuitive appeal of a "mosaic theory" in Fourth Amendment law,[16] it is not only wrong in principle but also impractical in application. Rather than resorting to an aggregation theory of the Fourth Amendment, this Note contends that the use of potentially invasive pattern-detecting technologies that are not

---

security, the mosaic theory suggests the potential for an adversary to deduce from independently innocuous facts a strategic vulnerability, exploitable for malevolent ends.

David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 630 (2005); *see also* 32 C.F.R. § 701.31 (2010) (defining the theory as "[t]he concept that apparently harmless pieces of information when assembled together could reveal a damaging picture"). The "mosaic theory" has been successfully invoked, often with merely perfunctory judicial review, by the government to justify a document's higher confidentiality classification or the withholding of documents through the Freedom of Information Act. *See, e.g.*, CIA v. Sims, 471 U.S. 159, 178–79 (1985) (holding that the CIA need not disclose the institutional affiliates of Agency-funded researchers who were previously held to be "intelligence sources"); Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice, 331 F.3d 918, 928–29 (D.C. Cir. 2003) (holding that the Department of Justice need not disclose information regarding persons detained in the wake of a major terrorist attack); N.J. Media Grp., Inc. v. Ashcroft, 308 F.3d 198, 217–20 (3d Cir. 2002) (denying media access to certain deportation hearings on the basis of national security); Hunt v. CIA, 981 F.2d 1116, 1118–20 (9th Cir. 1992) (denying request of an individual on trial for murder of Iranian national for CIA records pertaining to that national); Knight v. CIA, 872 F.2d 660, 663–64 (5th Cir. 1989) (holding the CIA exempt from disclosing documents relating to a sinking by French intelligence agents of a vessel belonging to an environmental and pacifist organization on the grounds that the material could compromise intelligence sources and methods); Halperin v. CIA, 629 F.2d 144, 150 (D.C. Cir. 1980) (protecting disclosure of legal bills and fee arrangements of private attorneys retained by the CIA); Halkin v. Helms, 598 F.2d 1, 8–9 (D.C. Cir. 1978) (invoking "mosaic theory" to support finding of state secrets privilege); *see also* Pozen, *supra*, at 630 (discussing the government's use of the theory to classify and withhold documents).

14 *See* Kerr, *supra* note 11; Sanchez, *supra* note 11.

15 The underlying premise of the "mosaic theory" has also been termed the "aggregation problem." *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1154 (2002).

16 *See* Sanchez, *supra* note 11 ("[T]here's an obvious intuitive appeal to the ["mosaic theory"], and indeed, we see that it fits our real world expectations about privacy much better than the cruder theory that assumes the sum of 'public' facts must always be itself a public fact.").

deemed "searches" in the first instance should be statutorily regulated. Part I examines the historical origins of the Fourth Amendment and tracks its treatment of electronic tracking devices. Part II discusses *Maynard* and the "mosaic theory," and ultimately suggests that the "mosaic theory" is inconsistent with existing Fourth Amendment precedent. Part III explores the far-reaching implications of the "mosaic theory" in Fourth Amendment law. Finally, Part IV contends that rather than regulating pattern-detecting technologies constitutionally at the aggregate level, privacy interests should be statutorily protected.

I. THE FOURTH AMENDMENT AND ELECTRONIC TRACKING DEVICES

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[17]

At its core, the Fourth Amendment protects individuals from arbitrary and intrusive official conduct.[18] The Fourth Amendment's mandates apply only to governmental conduct, which amounts to a "search" or "seizure" within the meaning of the Amendment.[19] Thus, defining what constitutes a search or a seizure within the meaning of the Fourth Amendment is of critical importance. Despite the Fourth

---

17 U.S. CONST. amend. IV.

18 *See* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 613–14 (1989) ("The Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government or those acting at their direction."); Camara v. Mun. Court, 387 U.S. 523, 528 (1967) ("The basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."); Berger v. New York, 388 U.S. 41, 53 (1967) ("The security of one's privacy against arbitrary intrusion by the police—which is at the core of the Fourth Amendment—is basic to a free society." (quoting Wolf v. Colorado, 338 U.S. 25, 27 (1949))); Schmerber v. California, 384 U.S. 757, 767 (1966) ("The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."); Johnson v. United States, 333 U.S. 10, 13–14 (1948) ("The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.").

19 *See* 1 JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE § 6.01[A] (5th ed. 2010).

Amendment's historical lineage, the term "search" has resisted a canonical formulation.[20] For years, the determination of what constituted a search was property-based.[21] That is, for the Fourth Amendment to be implicated, the government must have made a physical intrusion into a "constitutionally protected area."[22] Having difficulty applying this property-based approach to developing technologies,[23] the Supreme Court reformulated the Fourth Amendment search analysis in the seminal[24] case of *Katz v. United States*.[25]

Katz was convicted in federal court on a charge of interstate transmission of wagering information by telephone.[26] At trial, the court allowed the government to introduce incriminating evidence of the defendant's telephone conversations, which were overheard by FBI agents who had attached to the outside of a public phone booth an electronic listening and recording device.[27] On appeal, the Court

20 *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.1(a), at 430 (4th ed. 2004) ("The Supreme Court, quite understandably, has never managed to set out a comprehensive definition of the word 'searches' as it is used in the Fourth Amendment.").

21 *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 464–66 (1928) (holding that wire tapping of defendant did not amount to a search or seizure within the meaning of the Fourth Amendment as "there has been [no] official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure"), *overruled by* Katz v. United States, 389 U.S. 347, 353 (1967), *and Berger*, 388 U.S. 41; United States v. Lee, 274 U.S. 559, 563 (1927) (holding use of searchlight by boatswain not a search as "[t]here was [no] exploration below decks or under hatches"); Boyd v. United States, 116 U.S. 616, 630 (1886) ("[Fourth Amendment principles] apply to all invasions on the part of the government and its employés of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property . . . .").

22 Silverman v. United States, 365 U.S. 505, 512 (1961).

23 *See* 1 DRESSLER & MICHAELS, *supra* note 19, § 6.09[A] (noting that the Supreme Court shifted away from the property doctrine in *Katz* in large part because technological advances made the doctrine an inadequate limitation on governmental intrusion); *see also* Michael Goldsmith, *The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance*, 74 J. CRIM. L. & CRIMINOLOGY 1, 3 (1983) ("The question of electronic surveillance has long posed a classic confrontation between privacy interests and the need for effective law enforcement.").

24 *See* 1 DRESSLER & MICHAELS, *supra* note 19, § 6.03[A] ("*Katz v. United States* is the seminal case in modern 'search' law." (footnote omitted)); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 383 (1974) ("[*Katz*] is, of course, now generally recognized as seminal and has rapidly become the basis of a new formula of fourth amendment coverage.").

25 389 U.S. 347 (1967).

26 *See id.* at 348.

27 *See id.* at 348, 353.

held that the government's attachment and use of the electronic listening device was a "search and seizure" within the meaning of the Fourth Amendment.[28] In so holding, the Court moved away from the view that the scope of the Fourth Amendment "turn[ed] upon the presence or absence of a physical intrusion into any given enclosure,"[29] for "the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area.'"[30] Rather,

> the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[31]

In a concurring opinion, Justice Harlan provided the framework under which the Court would thereafter analyze Fourth Amendment searches—the "reasonable expectation of privacy" test.[32] Pursuant to this test, "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[33] Although *Katz* was hailed as a dramatic shift in Fourth Amendment law, it is not clear there was a profound divergence from the property-based approach.[34]

---

28 *See id.* at 353.

29 *Id.*

30 *Id.* at 350.

31 *Id.* at 351–52 (citations omitted).

32 *See id.* at 361 (Harlan, J., concurring).

33 *Id.* The inclusion of the first requirement in the test, that a person have an actual expectation of privacy, has been sharply criticized. *See* Amsterdam, *supra* note 24, at 384 ("An actual, subjective expectation of privacy obviously has no place in a statement of what *Katz* held or in a theory of what the fourth amendment protects. It can neither add to, nor can its absence detract from, an individual's claim to fourth amendment protection. If it could, the government could diminish each person's subjective expectation of privacy merely by announcing half-hourly on television . . . that we were all forthwith being placed under comprehensive electronic surveillance."). Justice Harlan, the author of the test, eventually agreed. *See* United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) ("The analysis must, in my view, transcend the search for subjective expectations or legal attribution of assumptions of risk."). Although the Court has never rejected the test, they have at times voiced caution in its application. *See* Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979) ("Situations can be imagined, of course, in which *Katz*' two-pronged inquiry would provide an inadequate index of Fourth Amendment protection.").

34 *See* 1 DRESSLER & MICHAELS, *supra* note 19, § 6.04[A][1] ("One can look almost in vain for a post-*Katz* ruling based on privacy that differs from the outcome one would expect from pre-*Katz* property-rights trespass analysis."); John M. Burkoff,

In *United States v. Knotts*,[35] the Supreme Court confronted the issue of whether the warrantless use of an electronic tracking device fell within the ambit of the Fourth Amendment.[36] In *Knotts*, Minnesota narcotics officers received information that codefendants Armstrong and Petschen were obtaining large amounts of chloroform—often used to manufacture illicit drugs—from a chemical company.[37] With the consent of the chemical company, the officers attached a beeper[38] inside a five-gallon container of chloroform, which the company was to give to the codefendants upon purchase.[39] After the purchase by Armstrong, officers followed the car by maintaining visual surveillance and by monitoring the signal emitted from the beeper.[40] During the codefendant's journey to respondent Knotts's secluded cabin in rural Wisconsin, Petschen's evasive maneuvers precluded the officers from maintaining visual surveillance.[41] With the assistance of a helicopter, the signal from the beeper was tracked to the cabin, where—after obtaining a search warrant—officers discovered a drug laboratory.[42] In reversing the Eighth Circuit, the Court held that the

When Is a Search Not a "Search?" Fourth Amendment Doublethink, 15 U. TOL. L. REV. 515, 529 (1984) ("[I]t is worth pointing out that the apparent reformulation of the fourth amendment's scope of application in *Katz* was not really so radical a proposition as the majority made it out to be. Traditionally protected property interests are surely among those areas of expectation generally, if not inevitably, included within the ambit of 'well-recognized Fourth Amendment freedoms.'" (footnote omitted)); Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1314 (2002) ("[The Supreme Court's] continued emphasis on property law again demonstrates that, notwithstanding the famous 'people, not places' language in the majority opinion, many courts properly reject the idea that *Katz* supplanted a 'place-based' analysis, since the location of the search and the defendant's relationship to that location are still a significant factor in determining whether or not the search was valid." (quoting *Katz*, 389 U.S. at 351)).

35 460 U.S. 276 (1983).

36 *See id.* at 277.

37 *See id.* at 278.

38 *See id.* at 277 ("A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver."); 1 LAFAVE, *supra* note 20, § 2.7(e) ("The police monitor the signals emitted by the beeper through the use of a receiver installed in a vehicle or airplane. By such monitoring, they are able to keep track of the movement of the object on which the beeper was placed, to ascertain the continued presence of that object within premises, or even to determine whether that object has been tampered with in a certain way.").

39 *See Knotts*, 460 U.S. at 278.

40 *See id.*

41 *See id.*

42 *See id.* at 278–79. According to the Court, nothing in the record indicated that the monitoring of the chloroform continued past the point in which the initial determination of its location at the cabin was made. *See id.* at 278–79, 284–85.

warrantless monitoring of the beeper was not a "search" within the meaning of the Fourth Amendment.[43] In so holding, the Court rejected the argument that the defendants had an expectation of privacy in their movements:

> A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When Petschen 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.[44]

Noting that the officers could have obtained the information through visual surveillance, the Court held that "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[45]

A year later in *United States v. Karo*,[46] the Court confronted the issue of whether the monitoring of a beeper in a private residence not open to visual surveillance is a search under the Fourth Amendment.[47] In *Karo*, the Drug Enforcement Administration (DEA) installed and subsequently monitored a beeper placed within a can of ether as it was transferred among several residences, a self-storage facility, and ultimately to a residence where the ether was being used to extract cocaine.[48] In holding the monitoring a search, the Court distinguished the case from *Knotts*[49] on the ground that the monitoring revealed information about the interior of the private residence—

---

43 *See id.* at 285.

44 *Id.* at 281–82.

45 *Id.* at 282; *see also id.* at 285 ("Admittedly, because of the failure of the visual surveillance, the beeper enabled the law enforcement officials in this case to ascertain the ultimate resting place of the chloroform when they would not have been able to do so had they relied solely on their naked eyes. But scientific enhancement of this sort raises no constitutional issues which visual surveillance would not also raise. A police car following Petschen at a distance throughout his journey could have observed him leaving the public highway and arriving at the cabin owned by respondent, with the drum of chloroform still in the car.").

46 468 U.S. 705 (1984).

47 *See id.* at 714.

48 *See id.* at 708–09.

49 *See Knotts*, 460 U.S. at 285 ("[T]here is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin.").

confirmation that the ether was actually within the residence and remained there until a warrant was obtained—that could not have otherwise been obtained absent a warrant, and such information was not voluntarily exposed.[50] Hence, "[i]ndiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."[51] Thus, after *Knotts* and *Karo*, the government is free to conduct sustained and prolonged surveillance of citizens as long as the monitoring is limited to movements in public areas.[52]

To date, the Supreme Court has yet to confront the issue of whether GPS[53] monitoring falls within the ambit of the Fourth Amendment. Several federal circuit courts of appeals, however, have held that GPS tracking in public areas is not a search.[54] In *United States v. Garcia*,[55] Judge Posner rejected the defendant's claim that the use of a GPS device is a search.[56] In so holding, he compared GPS devices to other non-searches, such as visual surveillance, cameras

50 *See Karo*, 468 U.S. at 715.

51 *Id.* at 716.

52 *See* 1 DRESSLER & MICHAELS, *supra* note 19, § 6.09[C] ("[T]he implication of *Knotts* is that as long as monitoring is limited to movements of persons in non-private areas, the government is free to conduct constant surveillance of citizens.").

53 *See* 1 LAFAVE, *supra* note 20, § 2.7 (Supp. 2007) ("Global Positioning System (GPS) devices used by law enforcement agencies are small, but usually larger than beepers. They contain not only a GPS satellite communications function that pinpoints the device's location. They also contain computerized recording devices, or logs. Law enforcement agents attach a GPS device to the underside of a vehicle, in a place where it will not be noticed. From then on the device automatically keeps a detailed time and place itinerary of everywhere the vehicle travels and when and how long it remains at various locations. Later, law enforcement agents remove the device and download the detailed itinerary of where and when the vehicle traveled. Unlike beepers, GPS devices do not require continuous monitoring by a law enforcement agent." (quoting Dorothy J. Glancy, *Privacy on the Open Road*, 30 OHIO N.U. L. REV. 295, 316–17 (2004))).

54 *See* United States v. Marquez, 605 F.3d 604, 609–10 (8th Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212, 1217 (9th Cir. 2010); United States v. Garcia, 474 F.3d 994, 997–98 (7th Cir. 2007). Like *Knotts*, all three courts reserved the question of whether mass surveillance of vehicular movements constituted a search under the Fourth Amendment. *See Marquez*, 605 F.3d at 610; *Pineda-Moreno*, 591 F.3d at 1217 n.2; *Garcia*, 474 F.3d at 998; *see also* United States v. Walker, No. 2:10-cr-32, 2011 WL 651414, at *3, *8 (W.D. Mich. Feb. 11, 2011) (rejecting the defendant's reliance on *Maynard*, noting that "the great weight of the law from other federal circuits rejects [*Maynard*'s] view")

55 474 F.3d 994 (7th Cir. 2007).

56 *See id.* at 996.

mounted on lampposts, and satellite imaging.[57] Conceding practical differences exist between visual surveillance and the other non-searches, Judge Posner concluded that "GPS tracking is on the same side of the divide with the surveillance cameras and the satellite imaging, and if what they do is not searching in Fourth Amendment terms, neither is GPS tracking."[58] In *United States v. Pineda-Moreno*,[59] the Ninth Circuit agreed, holding that the continuous monitoring of the defendant over a four-month period did not constitute a search within the meaning of the Fourth Amendment.[60] The court quickly dismissed the defendant's argument that *Kyllo v. United States*[61] heavily modified *Knotts*.[62] Thus, since "[t]he only information the agents obtained from the tracking devices was a log of the locations where [the defendant's] car traveled, information the agents could have obtained by following the car," the electronic tracking did not amount to a search.[63] Lastly, the Eighth Circuit in *United States v. Marquez*[64] stated in dicta that "when police have reasonable suspicion that a particular vehicle is transporting drugs, a warrant is not required when, while the vehicle is parked in a public place, they install a non-invasive GPS tracking device on it for a reasonable period of time."[65] Thus, prior to *Maynard*, every federal circuit court of appeals to confront the issue was consistent in holding that, pursuant to *Knotts*, the use of GPS devices to monitor the movements of individuals did not constitute a search.[66]

---

57 *See id.* at 997.

58 *Id.*

59 591 F.3d 1212 (9th Cir. 2010).

60 *See id.* at 1217.

61 533 U.S. 27, 34 (2001) (holding that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area'—constitutes a search—at least where (as here) the technology in question is not in general public use" (citation omitted) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961))).

62 *See Pineda-Moreno*, 591 F.3d at 1216–17.

63 *Id.* at 1216.

64 605 F.3d 604 (8th Cir. 2010).

65 *Id.* at 610. Although the Eighth Circuit agreed *Knotts* was controlling, the limitations the court placed on the use of GPS surveillance—reasonable suspicion of criminal activity and the use of the GPS device for a reasonable amount of time—are nowhere to be found in *Knotts* or any other federal circuit decision regarding the use of electronic tracking devices.

66 Two states have held electronic tracking to be a search under their respective state constitutional counterparts to the Fourth Amendment. *See* People v. Weaver, 909 N.E.2d 1195, 1199–1203 (N.Y. 2009) ("Under [article I, section 12 of the New York] Constitution, in the absence of exigent circumstances, the installation and use

II. *Maynard* and the "Mosaic Theory"

And then there was *Maynard*. In *Maynard*, the District of Columbia Circuit Court of Appeals held that the prolonged use of a GPS device to track the defendant twenty-four hours a day for four weeks constituted a search under the Fourth Amendment.[67] The court first addressed the question of whether *Knotts* was controlling.[68] In answering this question in the negative, the court relied upon a reservation left open in *Knotts*.[69] In *Knotts*, the respondent argued that the result of holding electronic tracking outside of the reach of the Fourth Amendment was that "twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision."[70] In response, the Court concluded that "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[71] With the questionable assertion that "dragnet-type law enforcement practices" refers to prolonged surveillance of a single individual, the *Maynard* court held that *Knotts* was not controlling.[72]

---

of a GPS device to monitor an individual's whereabouts requires a warrant supported by probable cause."); State v. Jackson, 76 P.3d 217, 222–24 (Wash. 2003) (holding that the installation and use of a GPS device on a private vehicle is a search under article I, section 7 of the Washington Constitution); *see also* Commonwealth v. Connolly, 913 N.E.2d 356, 366–69 (Mass. 2009) (holding the use of a GPS tracking device a seizure under article 14 of the Massachusetts Declaration of Rights). Oregon held the use of a radio transmitter to be a search under Article I, section 9, of the Oregon Constitution. *See* State v. Campbell, 759 P.2d 1040, 1049 (Or. 1988). In so holding, the Supreme Court of Oregon rejected defining searches in terms of "reasonable expectations of privacy." *Id.* at 1044. Although the electronic tracking device at issue in *Campbell* was a radio transmitter, it is likely that the court would characterize the use of a GPS tracking device as a search.

67 *See* United States v. Maynard, 615 F.3d 544, 555–56 (D.C. Cir. 2010).

68 *Id.* at 556.

69 *See id.*

70 United States v. Knotts, 460 U.S. 276, 283 (1983) (quoting Brief for Respondent at 9, *Knotts*, 460 U.S. 276 (No. 81-1802)).

71 *Id.* at 284.

72 *Maynard*, 615 F.3d at 556. It is questionable whether the *Knotts* reservation in fact referred to prolonged surveillance of a single individual. The three other federal circuit courts of appeals to decide the issue expressed the belief that the reservation was referring to mass surveillance. *See* United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212, 1217 n.2 (9th Cir. 2010); United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007). Another plausible view held by some commentators is that "dragnet-type law enforcement practices" meant the monitoring of private places. *See* Kerr, *supra* note 11. Although the reservation in *Knotts* was made in response to a claim that law enforcement agents would be able to continuously monitor individuals, the context of the case lends support to

The court then addressed whether the defendant's location pattern was exposed to the public.[73] The court first held that the totality of the defendant's movements was not exposed over the course of the month-long investigation.[74] The court reasoned that "unlike one's movements during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil."[75] Next, the court introduced the "mosaic theory" into Fourth Amendment law.[76] Relying on the "mosaic theory," the court

---

the latter interpretation. In *Knotts*, the Court repeatedly emphasized that the electronic tracking device was being used for the limited purpose of tracking the defendant in public areas and in no way intruded upon the sanctity of the home. *See Knotts*, 460 U.S. at 284–85. Although the *Maynard* court contends that *Knotts* distinguished between the use of a beeper to discover limited information from a discrete trip from information discovered through sustained monitoring, the language from *Knotts* used in support of this proposition clearly made no such distinction. *See Maynard*, 615 F.3d at 556. Rather, the distinction made in *Knotts* was between the limited information discovered through the use of the beeper in public areas, and information that would be discovered by such use in private areas. *See Knotts*, 460 U.S. at 284–85. Indeed, a year later in *Karo* it was the use of an electronic tracking device to monitor private areas—not the four-month continuous tracking of a can of ether—that was held to violate the Fourth Amendment. *See* United States v. Karo, 468 U.S. 705, 714 (1984).

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

74 *Id.*

75 *Id.*

76 *Id.* at 561–62. The "mosaic theory" is not novel with respect to state search and seizure law. Without labeling them as such, in holding that electronic tracking is a search under their respective state constitutions, *State v. Jackson*, 76 P.3d 217 (Wash. 2003), and *People v. Weaver*, 909 N.E.2d 1195 (N.Y. 2009), both make mosaic-type arguments. In *Jackson* the court stated:

> [T]he intrusion into private affairs made possible with a GPS device is quite extensive as the information obtained can disclose a great deal about an individual's life. . . . In this age, vehicles are used to take people to a vast number of places that can reveal preferences, alignments, associations, personal ails and foibles. The GPS tracking devices record all of these travels, and thus can provide a detailed picture of one's life.

Jackson, 76 P.3d at 223. Noting that the "inquiry under article I, section 7 is broader than that under the Fourth Amendment to the United States Constitution," it makes logical sense for the court to classify the "uninterrupted, 24-hour a day surveillance possible through use of a GPS device, which does not depend upon whether an officer could in fact have maintained visual contact," as a search under the state constitution. *Id.* at 222–23. In *Weaver*, the court stated:

> The whole of a person's progress through the world, into both public and private spatial spheres, can be charted and recorded over lengthy periods possibly limited only by the need to change the transmitting unit's batteries. . . . What the technology yields and records with breathtaking quality and quantity is a highly detailed profile, not simply of where we go, but by easy

concluded that the whole of Mr. Jones's movements was not constructively exposed.[77] The court reasoned:

> The whole of one's movements over the course of a month is not constructively exposed to the public because, like a rap sheet, that whole reveals far more than the individual movements it comprises. The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, not the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more.[78]

In other words, "[p]rolonged 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."[79] Thus, according to the "mosaic theory," although the individual acts are exposed and are therefore not rendered searches, the acts viewed collectively become a search.[80]

Beyond the *Maynard* court's questionable treatment of the "dragnet-type law enforcement practices" reservation in *Knotts*,[81] the opinion is inconsistent with existing Fourth Amendment jurisprudence in

---

> inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our professional and avocational pursuits.

Weaver, 909 N.E.2d at 1199–1200. In fact, the Colorado Supreme Court explicitly used the "mosaic theory" to hold the use of a pen register a search under the Colorado Constitution. *See* People v. Sporleder, 666 P.2d 135, 141–42 (Colo. 1983). The court held:

> The pen register recorded each telephone number dialed by the defendant as well as the date and time of each telephone call. Knowledge of these facts can often yield inferential knowledge of the content of the conversation itself. In addition, a pen register record holds out the prospect of an even greater intrusion in privacy when the record itself is acquired by the government, which has a technological capacity to convert basic data into a virtual mosaic of a person's life.

Id.

77 *See Maynard*, 615 F.3d at 561–62.

78 *Id.*

79 *Id.* at 562.

80 *But see* UNITED STATES v. JONES, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, C.J., dissenting from the denial of rehearing en banc) ("The reasonable expectation of privacy as to a person's movements on the highway is, as concluded in *Knotts*, zero. The sum of an infinite number of zero-value parts is also zero.").

81 *See supra* note 72 and accompanying text.

at least two respects.[82] First, *Maynard* conflicts with the Supreme Court's voluntary exposure analysis. The Court has often classified theoretical or limited disclosures of information as complete exposures warranting no Fourth Amendment protection.[83] In fact, the *Maynard* court's holding that "the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil" was implicitly rejected in *Knotts*. In *Knotts*, it was practically impossible for an individual to observe the whole of the defendant's interstate movements—the defendants had in fact evaded the visual surveillance of the law enforcement and bystanders would have observed only a fraction of the whole trip.[84] That is, although an individual bystander may have viewed codefendants Armstrong and Petschen at mile ten of their journey, that particular bystander would not have known that the automobile contained a container of chloroform or that the vehicle and container would come to rest at Knotts's cabin. This was irrelevant, however, for the purposes of the exposure analysis.[85] Although

82 SEE JONES, 625 F.3d at 767 (Sentelle, C.J., dissenting from the denial of rehearing en banc) ("[*Maynard*] is inconsistent not only with every other federal circuit which has considered the case, but more importantly, with controlling Supreme Court precedent set forth in [*Knotts*].").

83 *See* 2 CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING & EAVESDROPPING § 30:19 (3d ed. 2007) ("[A]ny 'knowing exposure' of information to the public in effect waives Fourth Amendment protection from purposeful police surveillance of a similar kind, even if the exposure in question is far more theoretical than real."); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 566 (1990) ("[T]he Supreme Court has frequently denied Americans fourth amendment protection for information disclosed for limited use on the theory that this disclosure amounts to a complete renunciation of any privacy interest in that information."); Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 LAW & CONTEMP. PROBS. 125, 133–34 (2002) (noting that the Court's "framework . . . readily finds that suspects 'assume the risk' that *any* information disclosure becomes a revelation to many or all").

84 *See* United States v. Knotts, 460 U.S. 276, 278–79 (1983).

85 *See* 1 DRESSLER & MICHAELS, *supra* note 19, § 6.09[C] ("The implication of *Knotts* is that as long as it is hypothetically conceivable (although, in some cases, nearly impossible practically) to obtain information in a non-technologically-enhanced manner from a lawful vantage point, it is irrelevant that, instead, the government uses an electronic tracking device to obtain the same information."); Wayne R. LaFave, *The Fourth Amendment Today: A Bicentennial Appraisal*, 32 VILL. L. REV. 1061, 1082 (1987) ("But to learn what the beeper revealed—that chemicals purchased in Minneapolis were now in a particular secluded cabin 100 miles away—would have taken an army of bystanders in ready and willing communication with one another."); Silas J. Wasserstrom, *The Incredible Shrinking Fourth Amendment*, 21 AM. CRIM. L. REV. 257, 376 (1984) ("Electronic monitoring of a car, however, enables the police to trace its every movement, day and night, for an extended period of time, something they

"in ordinary life, we often reasonably suppose the privacy or secrecy of certain facts . . . that could *in principle* be inferred from the combination of other facts that are (severally) clearly public, because it would be highly unusual for all of them to be observed by the *same* public,"[86] such facts are not given Fourth Amendment protection under *Knotts*. While it is true that the surveillance in *Knotts* was conducted over one trip spanning a day, it is not clear why under *Knotts*'s analysis continuous surveillance would be treated any differently. Thus, pursuant to *Knotts*, an expectation of privacy does not exist "as to the aggregate of information disclosed only in fragments to hypothetical bystanders."[87] This principle was not altered by *Karo*.[88]

Second, the Supreme Court has on multiple occasions implicitly rejected the proposition that the Fourth Amendment analysis is altered when an investigatory technique is prolonged to the point where information may be accumulated. In *Smith v. Maryland*,[89] the Court recognized that a pen register may be used to examine permanent or lengthy phone records, but rejected arguments[90] that this fact implicated the Fourth Amendment because the record of phone numbers dialed would reveal intimate details of an individual's life.[91] In addition, it is particularly noteworthy that in *Karo*, the prolonged duration of the electronic tracking—spanning several months—played no role in holding the use a search.[92]

---

could accomplish by visual surveillance, if at all, only by assigning a small army of agents to the task.").

86 Sanchez, *supra* note 11.

87 1 LAFAVE, *supra* note 20, § 2.7(e), at 763.

88 *See id.*

89 442 U.S. 735 (1979).

90 *See id.* at 748 (Stewart, J., dissenting) ("The numbers dialed from a private telephone—although certainly more prosaic than the conversation itself—are not without 'content.' . . . I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and places called, and thus reveal the most intimate details of a person's life."); *id.* at 751 (Marshall, J., dissenting) ("The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts.").

91 *See id.* at 745–46 (majority opinion).

92 *See* United States v. Karo, 468 U.S. 705, 708–10, 715 (1984).

III. IMPLICATIONS OF THE "MOSAIC THEORY" IN FOURTH AMENDMENT LAW

The application of the "mosaic theory" to the Fourth Amendment would not only be wrong in principle, it would be impractical in application. *Maynard* is steeped in uncertainty as to the effects of the Fourth Amendment's recognition of an aggregation theory of searches. In articulating a novel theory of Fourth Amendment law, *Maynard* lacks an accompanying elucidation of the manner in which the theory functions in the Fourth Amendment. *Maynard* left little guidance as to the determination of the proper scope of the mosaic, whether the theory would implicate other pattern-detecting investigatory techniques, and the appropriate standard of judicial review.

A. The Creation and Scope of the Mosaic

Maynard left little guidance as to what durational threshold must to be crossed in order for the use of pattern-detecting technology to be sufficiently prolonged as to render it a search.[93] Without a clearly demarcated line, law enforcement agents, judges, and individuals cannot know when an aggregate of information will receive Fourth Amendment protection. Law enforcement agents are left to speculate as to how much is too much.[94] This lack of clarity will deter law enforcement agents from utilizing the full extent of their investigatory power. This is even more problematic with respect to the "mosaic theory's" creation of retroactive unconstitutionality.[95] As soon as a pat-

93 *See* United States v. Sparks, No. 10-10067-WGY, slip op. at 9 (D. Mass. Nov. 10, 2010) (rejecting *Maynard*'s aggregation approach as it "leaves police officers with a rule that is vague and unworkable. It is unclear when surveillance becomes so prolonged as to have crossed the threshold and created this allegedly intrusive mosaic."); Kerr, *supra* note 11 ("Much of the problem is knowing when the line is crossed when a bunch of non-searches become a search."); Sanchez, *supra* note 11 (calling the question of when "individual instances of permissible monitoring become a search requiring judicial approval" a "thorny" one).

94 *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 883–84 (2004) ("[I]nterstitial rulemaking that leaves the rules unclear lessens the clarity of the limits on the government's powers to invade privacy, underdeterring police behavior in some contexts and overdeterring it in others."); *id.* at 861 ("[T]he rules [of criminal procedure] tell government agents what they can and cannot do to collect evidence of crime and identify wrongdoers. Because these rules limit government power, rule clarity minimizes official discretion and encourages compliance. Unclear rules mean unclear limits on government power, increasing the likelihood of abuses by aggressive government officials.").

95 *See Sparks*, No. 10-10067-WGY, slip op. at 9 (recognizing that under *Maynard*'s aggregation approach "conduct that is initially constitutionally sound could later be

tern is created, previously permissible individual law enforcement steps become unconstitutional. Because the "mosaic theory" retroactively renders the entire mosaic unconstitutional and subject to suppression, law enforcement agents will be even more hesitant in exercising the full extent of their investigatory power.

Further, if the "mosaic theory" in the Fourth Amendment is premised on the idea that "prolonged GPS monitoring reveals an intimate picture of the subject's life that he expects no one to have—short perhaps of his spouse,"[96] who has the burden of proof with respect to whether the prolonged surveillance has in fact revealed an intimate picture of an individual's life and thus created a mosaic? Unless the location of a "stash-house" is an intimate detail, *Maynard* can be read to stand for the proposition that warrantless prolonged GPS surveillance is per se unconstitutional. Such an approach would be over-inclusive in that prolonged location monitoring that does not result in a pattern, or a pattern that does not reveal intimate details, would be rendered a search within the meaning of the Fourth Amendment and therefore subject to suppression.

Once the mosaic threshold is crossed and a mosaic is created, the question that arises is to how to define the scope of the mosaic. If law enforcement officials engage in a number of sustained investigatory techniques—as they often do—it is likely that whole investigations will be called into question. That is, if a pattern is detected only through the use of multiple investigatory techniques, and the theory is applied consistently, the investigation in its entirety will be rendered a search.[97] In this respect, the retroactive effect of the "mosaic theory" takes on greater significance. Rather than having the entire investigation held inadmissible and subject to suppression, law enforcement agents will be overly cautious as to the amount of surveillance conducted. The lack of clarity as to how prolonged the surveillance must be to render it a search, whether intimate details need in fact emerge, and what the proper scope of the mosaic is will provide defendants with an arsenal to attack every police investigation.

---

deemed impermissible if it becomes part of the aggregate"); Kerr, *supra* note 11 ("[T]he mosaic theory has the bizarre consequences of creating retroactive unconstitutionality.").

96 United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010).

97 *See* Kerr, *supra* note 11 ("[I]f the Fourth Amendment recognizes a mosaic theory, then the Fourth Amendment will regulate entire investigations as a whole: The question will be whether the investigation measured *in the aggregate* amounts to a Fourth Amendment violation.").

B. Implication of Previously Accepted Investigatory Techniques

One of the most serious implications of the "mosaic theory" in Fourth Amendment law is that it calls into question the validity of previously accepted forms of surveillance. GPS surveillance is not the only form of surveillance that provides law enforcement with a comprehensive and detailed record of someone's movements or affairs when it is sustained on a prolonged basis. Thus, the "mosaic theory," which focuses on the resulting patterns created by individual law enforcement acts that in and of themselves are not searches, naturally calls into question other accepted investigative techniques that are performed on a sufficiently prolonged basis.[98] For instance, the "mosaic theory" calls into question the use of pen registers[99] and trap and trace devices,[100] which have been held to not implicate the Fourth Amendment.[101] The "mosaic theory" would also seemingly

98 SEE United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, C.J., dissenting from the denial of rehearing en banc) ("[I]t would appear . . . that this novel aggregation approach to the reasonable expectation of privacy would prohibit not only GPS-augmented surveillance, but any other police surveillance of sufficient length to support consolidation of data into the sort of pattern or mosaic contemplated by the panel.").

99 *See* 18 U.S.C. § 3127(3) (2006) ("[T]he term 'pen register' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business."). Relying on a "mosaic theory" argument, the Colorado Supreme Court held the warrantless use of pen registers unconstitutional under the Colorado constitutional counterpart to the Fourth Amendment. *See* People v. Sporleder, 666 P.2d 135, 141–42 (Colo. 1983); *see also* 1 LAFAVE, *supra* note 20, § 2.7 ("The use of . . . pen registers . . . often results in the discovery of one's continuing associations with other persons.").

100 *See* 18 U.S.C. § 3127(4) ("[T]he term 'trap and trace device' means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communications.").

101 *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that the Fourth Amendment does not prohibit the warrantless installation and use of a pen register). Although law enforcement use of pen registers and trap and trace devices do not implicate the Fourth Amendment, ex ante judicial approval is statutorily mandated. *See infra* note 151 and accompanying text.

implicate the prolonged use of a mail cover[102] as an investigatory technique.[103] Although the Supreme Court has yet to address the issue, courts have held that the warrantless use of a mail cover does not violate the Fourth Amendment.[104] Another accepted investigatory technique that can reveal very intimate details of an individual's life—particularly if sustained for a prolonged basis—is garbage inspections.[105] It could plausibly be argued that the patterns that result from the prolonged use of garbage inspections are much more intrusive than any pattern resulting from the use of a GPS device.[106] The same could be said about prolonged video surveillance.[107] It is well

102 *See* 39 C.F.R. § 233.3(c)(1) (2010) ("*Mail cover* is the process by which a nonconsensual record is made of any data appearing on the outside cover of any sealed or unsealed class of mail matter, or by which a record is made of the contents of any unsealed class of mail matter as allowed by law, to obtain information in order to: (i) Protect national security, (ii) Locate a fugitive, (iii) Obtain evidence of commission or attempted commission of a crime, (iv) Obtain evidence of a violation or attempted violation of a postal statute, or (v) Assist in the identification of property, proceeds or assets forfeitable under law."); *see also id.* § 233.3(c)(6) ("*Crime*, for the purposes of [§ 233.3], is any commission of an act or the attempted commission of an act that is punishable by law or by imprisonment for a term exceeding one year.").

103 *See* 1 LAFAVE, *supra* note 20, § 2.7(a) ("One investigative technique which is employed to determine the relationships and associations of a person and to obtain leads into other details of his life is the mail cover." (footnotes omitted)).

104 *See, e.g.*, United States v. Choate, 576 F.2d 165, 177 (9th Cir. 1978) (holding that the use of mail covers to obtain information from the exterior of an individual's mail does not violate the Fourth Amendment given that "the information would foreseeably be available to postal employees"). Like pen registers and trap and trace devices, although the use of mail covers does not fall within the ambit of the Fourth Amendment, its use as an investigative technique is statutorily governed. *See infra* note 152 and accompanying text.

105 *See* California v. Greenwood, 486 U.S. 35, 37 (1988) (holding that the Fourth Amendment does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of the home).

106 *See id.* at 50 (Brennan, J., dissenting) ("A single bag of trash testifies eloquently to the eating, reading, and recreational habits of the person who produced it. A search of trash, like a search of the bedroom, can relate intimate details about sexual practices, health, and personal hygiene. Like rifling through desk drawers or intercepting phone calls, rummaging through trash can divulge the target's financial and professional status, political affiliations and inclinations, private thoughts, personal relationships, and romantic interests."); 1 LAFAVE, *supra* note 20, § 2.6(c) ("[O]ne's trash may expose 'intimate areas of an individual's personal affairs' and 'can reveal much about a person's activities, associations, and beliefs.'" (quoting Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 78–79 (1974) (Powell, J., concurring))).

107 *See* Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1409 (2004) (noting in the context of video surveillance that "even where a person does not worry about a particular action being observed in isolation, such actions may reveal private thoughts or goals when viewed in the aggregate").

settled that video surveillance in public areas does not give rise to a Fourth Amendment issue.[108] Thus, video cameras may be placed outside of an individual's residence, and so long as the cameras are incapable of viewing the interior of the residence, no Fourth Amendment right is infringed upon.[109]

Since *Maynard*, the "mosaic theory" has in fact been used as the basis for holding a previously accepted investigatory technique a search. In *In re Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information*,[110] Magistrate Judge Orenstein denied the government's application for an order under the Stored Communications Act[111] directing a service provider to disclose two months worth of historical cell-site location information.[112] According to Magistrate Judge Orenstein:

> The *Maynard* court's concern with sustained GPS tracking over the course of a month was not its formally continuous nature, but rather the fact that it results in a vast collection of specific data points that, viewed together, convey the "intimate picture" of a subject's life. It is the ability to amass a collection of such points, and not the ability to trace the route from each one to the next, that carries with it the ability to resolve those points into a comprehensible picture.[113]

Applying the "mosaic theory" to historical cell-site information, Magistrate Judge Orenstein concluded that the Fourth Amendment required the government to obtain a warrant based on a showing of probable cause.[114]

The most significant implication of the "mosaic theory," however, is that it calls into question the governmental use of prolonged visual

---

108 *See* 2 FISHMAN & MCKENNA, *supra* note 83, § 30:24(a); 1 LAFAVE, *supra* note 20, § 2.7(f).

109 *See* 2 FISHMAN & MCKENNA, *supra* note 83, § 30:24(a); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 236 (2002).

110 736 F. Supp. 2d 578 (E.D.N.Y. 2010).

111 18 U.S.C. §§ 2701–2712 (2006 & Supp. III 2009).

112 *See In re Application of the United States of America*, 736 F. Supp. 2d at 579.

113 *Id.* at 595; *see also In re* Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, No. 10-MC-0897 (JO), 2010 WL 5437209, at *3 (E.D.N.Y. Dec. 23, 2010) ("Location information is not a simple business record and, as convincingly explained in *Maynard*, it can effectively convey details that reveal the most sensitive information about a person's life-information that goes far beyond the ordinary course of the service provider's business.").

114 *See In re Application of the United States of America*, 736 F. Supp. 2d at 579.

surveillance in criminal investigations.[115] In *Maynard*, the court addressed the issue of the possible extension of the "mosaic theory" to prolonged visual surveillance.[116] Although the court ultimately declined to decide whether such a situation would constitute a search under the new theory, it suggested that visual surveillance would not be implicated.[117] The court noted that practically, law enforcement agents do not have the capability to sustain visual monitoring for a duration that exposes information not revealed to the public.[118] This argument is unpersuasive to the extent that it suggests that a mosaic is only created if the whole of one's movements is captured. A pattern can be created, and thus intimate details revealed, by the aggregation of individual law enforcement steps not necessarily constituting the whole of the investigatory techniques employed. The court implicitly recognizes this, as even continuous GPS tracking of a vehicle does not reveal the entirety of one's movements, but rather only the movements of a particular vehicle. Further, the dismissal of the implication of visual surveillance is problematic to the extent that it relies on the probability of law enforcement success. Such probability, however, must be viewed in relation to the factual context in which the investigation is conducted, and not in the abstract. To be sure, it is not beyond the realm of possibility that a properly equipped and resourced law enforcement unit would be capable of monitoring an unsuspecting individual for a continuous period of time sufficient to create a mosaic.

As a theoretical matter, the court reasoned that in contrast to prolonged GPS monitoring, the extension of the "mosaic theory" to visual surveillance would fail as the means used to uncover private

115 SEE United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, C.J., dissenting from the denial of rehearing en banc) ("I cannot discern any distinction between the supposed invasion by aggregation of data between the GPS-augmented surveillance and a purely visual surveillance of substantial length."); United States v. Sparks, No. 10-10067-WGY, slip op. at 9 (D. Mass. Nov. 10, 2010) ("[A] rule prohibiting prolonged GPS surveillance due to the quantity or quality of information it accumulates would also incidentally outlaw warrantless visual surveillance."); *see also* 1 LAFAVE, *supra* note 20, § 2.7(f) ("A moving surveillance may be conducted, either briefly or as long as several months, in order to determine if a particular individual is engaged in criminal activity or—more likely—to identify all of the participants in an ongoing criminal conspiracy.").

116 *See* United States v. Maynard, 615 F.3d 544, 565 (D.C. Cir. 2010).

117 *See id.*

118 *See id.* The court also applied this reasoning to video surveillance, where according to the court "photographic surveillance would require a net of video cameras so dense and so widespread as to catch a person's every movement, plus the manpower to piece the photographs together." *Id.*

information would not defeat one's expectation of privacy.[119] The court's analogy to the distinction between the placement of undercover agents and wiretapping[120] overlooks the fact that here, warrantless GPS tracking and visual surveillance are constitutional in the first instance. In fact, the "mosaic theory" focuses on the nature of the information revealed—a pattern exposing intimate details—and does not focus on the investigatory method used to attain such information. Beyond prolonged visual and video surveillance, *Maynard* does not express a view as to whether other investigatory techniques would be called into question by the "mosaic theory." This analysis suggests that the "mosaic theory," if consistently applied, would implicate the cumulative effect of previously accepted surveillance methods.[121] It is in this capacity that the "mosaic theory" has the potential to revolutionize the Fourth Amendment.

C. *Standard for Issuance*

A question left open in *Maynard* is what standard of review is necessary for the use of pattern-detecting investigatory techniques in criminal investigations. That is, in holding that the prolonged use of pattern-detecting technology was a search, the court failed to specify what kind of review would be sufficient. Thus, by saying that this type of investigative technique is more than just the use of a tracking device and that the prolonged surveillance is more intrusive and necessitates some kind of review, the question clearly becomes what kind of review is necessary. By failing to provide such guidance, the *Maynard* court left law enforcement agents to speculate as to what information they must provide to obtain authorization and left courts to speculate as to where on the spectrum of judicial review this heightened surveillance falls.

---

119 *See id.* at 566.

120 *See id.*

121 Judge Posner's analysis of GPS tracking in *Garcia* supports the conclusion that the "mosaic theory" will, if applied consistently to all investigatory techniques that result in a pattern, affect other accepted investigatory methods. In deciding that GPS tracking was not a search within the meaning of the Fourth Amendment, Judge Posner stated that "GPS tracking is on the same side of the divide with the surveillance cameras and the satellite imaging, and if what they do is not searching in Fourth Amendment terms, neither is GPS tracking." United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007). In the converse, if the prolonged use of a GPS tracking device results in a search because it creates a mosaic, the prolonged use of surveillance cameras and satellite imaging should accordingly be characterized as searches, provided of course that a pattern emerged from the aggregation of individual uses.

By categorizing the retrieval of digital location patterns as a search, it does not necessarily follow that the absence of a warrant based on probable cause[122] renders the search unconstitutional. The *Maynard* court left open the question of "whether, absent a warrant, either reasonable suspicion or probable cause would have been sufficient to render the use of the GPS lawful."[123] Although the Supreme Court has repeatedly emphasized that searches absent a warrant based upon a standard of probable cause are generally unreasonable,[124] today many searches require less than probable cause to be justified.[125] In *Terry v. Ohio*,[126] the Court imported a reasonableness test—first articulated by the Court in the administrative search case of *Camara v. Municipal Court*[127]—into criminal investigations. Pursuant to this balancing test, in order to assess an officer's conduct,

> as a general proposition, it is necessary "first to focus upon the governmental interest which allegedly justifies official intrusion upon the constitutionally protected interests of the private citizen," for there is "no ready test for determining reasonableness other than by balancing the need to search [or seize] against the invasion which the search [or seizure] entails."[128]

---

122 *See* Illinois v. Gates, 462 U.S. 213, 238 (1983) ("The task of the issuing magistrate is simply to make a practical, commonsense decision whether, given all the circumstances set forth in the affidavit before him . . . , there is a fair probability that contraband or evidence of a crime will be found in a particular place."); Brinegar v. United States, 338 U.S. 160, 175 (1949) ("In dealing with probable cause, however, as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act. The standard of proof is accordingly correlative to what must be proved."); 1 DRESSLER & MICHAELS, *supra* note 19, § 8.02[A] ("'Probable cause' exists when the facts and circumstances within an officer's personal knowledge, and of which he has reasonably trustworthy information, are sufficient in themselves to warrant a person of reasonable caution in the belief that . . . in the case of a search, a specifically described item subject to seizure will be found in the place to be searched.").

123 UNITED STATES v. JONES, 625 F.3d 766, 767 (D.C. Cir. 2010) (Ginsburg, Tatel & Griffith, JJ., concurring in the denial of rehearing en banc).

124 *See, e.g.*, Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 665 (1989) (emphasizing that while "a search must be supported, as a general matter, by a warrant issued upon probable cause . . . neither a warrant nor probable cause . . . is an indispensable component of reasonableness in every circumstance").

125 *See* 1 DRESSLER & MICHAELS, *supra* note 19, § 8.06; Burkoff, *supra* note 34, at 542; Solove, *supra* note 15, at 1119; Wasserstrom, *supra* note 85, at 309.

126 392 U.S. 1 (1968).

127 387 U.S. 523 (1967).

128 *Terry*, 392 U.S. at 20–21 (alterations in original) (quoting *Camara*, 387 U.S. at 534–35, 536–37).

Thus, if the balance weighs in favor of the search, a search may be justified notwithstanding the absence of probable cause.[129] Although *Camara* dealt with administrative searches and *Terry* with investigatory stops, this reasonableness approach has been extended to other search and seizure contexts[130]—including searches in public areas.[131] Under this reasonableness approach, many warrantless searches have been justified on the basis of reasonable suspicion, rather than probable cause.[132] Furthermore, a number of searches have likewise been upheld as reasonable in the absence of suspicion of any kind.[133]

Even if an ex post reasonableness test is ultimately rejected, it does not follow that the warrant must be issued only on probable cause.[134] If the use of pattern-detecting investigatory methods is viewed as overly intrusive, a heightened standard above probable cause may be warranted. Title III of the Omnibus Crime Control and

---

129 *See id.*; *see also* OTIS H. STEPHENS & RICHARD A. GLENN, UNREASONABLE SEARCHES AND SEIZURES 143 (2006) ("Today, under a vast array of circumstances, warrantless searches and seizures are nevertheless reasonable, at least in the opinion of the nation's highest court.").

130 *See* THOMAS N. MCINNIS, THE EVOLUTION OF THE FOURTH AMENDMENT 153 (2009); LaFave, *supra* note 85, at 1070–71.

131 *See* BRUCE A. NEWMAN, AGAINST THAT "POWERFUL ENGINE OF DESPOTISM" 102 (2007) ("[I]n the cases involving searches in public areas that have reached the Court, it has ruled that the reasonableness clause, not the warrant clause, is controlling.").

132 *See, e.g.*, Maryland v. Buie, 494 U.S. 325, 327 (1990) (protective residence sweeps); O'Connor v. Ortega, 480 U.S. 709, 725–26 (1987) (search of public employee); New Jersey v. T.L.O., 469 U.S. 325, 341 (1985) (search of public school students); *see also* 1 DRESSLER & MICHAELS, *supra* note 19, § 8.07[C][1] ("[S]ome searches may be conducted on a lesser level of suspicion than probable cause.").

133 *See, e.g.*, Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 664–65 (1995) (drug testing of public school students); Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990) (highway sobriety checkpoint); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 616–18 (1989) (drug and alcohol testing of public employees); United States v. Ramsey, 431 U.S. 606, 616 (1977) (border searches); South Dakota v. Opperman, 428 U.S. 364, 373–76 (1976) (car inventory searches); *see also* 1 DRESSLER & MICHAELS, *supra* note 19, § 8.07[C][1] ("[I]n a few circumstances, where the intrusion on privacy is especially slight, and society's interest in conducting the search or seizure is unusually great, government officers may act without *any* individualized suspicion.").

134 *See* Katz, *supra* note 83, at 584 n.124 (proposing electronic tracking be classified as intrusions and be subjected to an intermediate standard of reasonable suspicion); Slobogin, *supra* note 109, at 218 (contending that "given its relatively unintrusive nature, most public surveillance of individuals does not require probable cause in the traditional sense"). *But see* Thomas C. Marks, Jr. & Robert Batey, *Electronic Tracking Devices: Fourth Amendment Problems and Solutions*, 67 KY. L.J. 987, 1002 (1979) (contending that, in the context of electronic tracking devices, "probable cause to believe the monitored item is being used in ongoing criminal activity . . . seems to be the best standard for determining whether a warrant should issue").

Safe Streets Act provides for extraordinary review of electronic surveillance, with full probable cause, and alternative mechanisms.[135] Title III, as amended by Title I of the Electronic Communications Privacy Act of 1986 (ECPA),[136] regulates the interception of wire, oral, and electronic communications.[137] The requirements for an interception order are more onerous than what would be required under the Fourth Amendment.[138] Title III excempts from the definition of "electronic communication" "any communication from a tracking device (as defined in § 3117 of [Title 18])."[139] It could be argued that the digital location patterns are something different, something more intrusive than electronic tracking devices, and thus should be read to fall within the meaning of "electronic communication" under § 2510(12). This, however, does not seem plausible as the definition of "electronic communication" excludes "any communication from a tracking device,"[140] thus foreclosing the argument that although the interception of the digital location pattern was derived from the use

135 *See* 18 U.S.C. §§ 2510–2522 (2006 & Supp. III 2009).

136 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 101–111, 100 Stat. 1848, 1848–59 (codified as amended at 18 U.S.C. §§ 2510–2522).

137 *See* 18 U.S.C. §§ 2510–2522.

138 The interception order must be authorized by a high-level Department of Justice official and signed by a federal judge. *See* 18 U.S.C. § 2516 (2006). 18 U.S.C. § 2518(3) provides the probable cause showing that must be made:

(3) Upon such application the judge may enter an ex parte order . . . if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; . . .

(d) except as provided in [18 U.S.C. § 2518(11)], there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

Id. § 2518(3). In addition, the judge must also determine on the basis of the facts that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." *Id.* § 2518(3)(c). Further, the interception must "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under [Title III]." *Id.* § 2518(5). Finally, any Title III order is time-limited to thirty days, although the government can request an extension. *See id.* § 2518(5).

139 *Id.* § 2510(12)(C).

140 *Id.*

of an electronic tracking device, it was nonetheless governed by the mandates of Title III.[141]

Even though Title III will likely be held not to govern a request for digital location patterns, courts could still analyze such requests under the mandates of Title III. Although the plain language of Title III appears to exclude the interception of location patterns arising out of the use of tracking devices, courts could still use Title III as a guide for the constitutional standard. The adoption of the Title III standards to a type of surveillance not covered by Title III is not novel. In *United States v. Torres*,[142] Judge Posner held that, in the absence of statutory regulations governing the issuance of warrants for private video surveillance, the federal government may conduct video surveillance of the interior of a private building if the warrant under which the surveillance was conducted complied with the statutory mandates of Title III.[143] Although Title III did not govern video surveillance, the "exceedingly intrusive" and "inherently indiscriminate" nature of the private video surveillance compelled the adoption of the statutory mandates of Title III as a guide for the issuance of warrants authorizing private video surveillance.[144] Thus, in the absence of statutory regulations governing the issuance of warrants for pattern-detecting technologies, if the surveillance is of a highly intrusive and indiscrimi-

141 *Id.* § 3117(b) defines the term "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." *Id.* § 3117(b).

142 751 F.2d 875 (7th Cir. 1984).

143 *See id.* at 884–85.

144 *See id.* at 882. Other federal courts have likewise adopted the mandates of Title III in the private video surveillance context. *See* United States v. Williams, 124 F.3d 411, 416 (3d Cir. 1997); United States v. Falls, 34 F.3d 674, 680 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 1992); United States v. Mesa-Rincon, 911 F.2d 1433, 1438 (10th Cir. 1990); United States v. Cuevas-Sanchez, 821 F.2d 248, 252 (5th Cir. 1987); United States v. Biasucci, 786 F.2d 504, 510 (2d Cir. 1986); *see also* 2 FISHMAN & MCKENNA, *supra* note 83, § 30:25 (calling the adoption of Title III requirements in the video surveillance context "plausible and sensible," but criticizing the courts' treatment of such applications as constitutionally mandated); Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1433–37 (2002) (proposing legislative enactment of Title III-like standards for enhanced visual surveillance). *But see* Ric Simmons, *Can* Winston *Save Us from Big Brother? The Need for Judicial Consistency in Regulating Hyper-Intrusive Searches*, 55 RUTGERS L. REV. 547, 589 (2003) (criticizing this practice in the belief that courts "have relinquished their judicial duty to interpret the Constitution, an abdication which . . . is especially problematic when it occurs in the context of surveillance techniques that are both extraordinarily intrusive and becoming more common and more technologically sophisticated with every year").

nate nature, the adoption of the heightened requirements of Title III may be warranted.

On the other end of the spectrum, after concluding that this type of surveillance is a search, a standard less than probable cause may be deemed appropriate.[145] For instance, if the use of pattern-detecting investigatory techniques is not viewed as overly intrusive, a standard of reasonable suspicion could govern the issuance of a court order.[146] In *Karo*, the government argued that if the electronic monitoring was a search, a warrant should issue on a showing of reasonable suspicion rather than probable cause.[147] The Court declined to decide the issue, stating that "[i]t will be time enough to resolve the probable cause-reasonable suspicion issue in a case that requires it."[148] If the Fourth Amendment did require a warrant to issue upon probable cause, the Court would have had no problem dismissing the government's contention. Instead, the Court reserved the issue for another day. By doing so, it gave substance to the argument that a warrant may issue on less than probable cause.

IV. STATUTORY PROTECTION

Given the inconsistency with existing Fourth Amendment law and the impracticality of its application, the "mosaic theory" should be rejected in Fourth Amendment law.[149] The unrestricted use of pattern-detecting devices, however, would have a substantial and deleterious effect on privacy. A response to this threat, therefore, should be

145 *See* United States v. Michael, 645 F.2d 252, 258 (5th Cir. 1981) (holding, before *Knotts*, that regardless of whether the attachment and monitoring of an electronic tracking device was a search, reasonable suspicion justified such use); *see also* United States v. Moore, 562 F.2d 106, 113 n.3 (1st Cir. 1977) (concluding that probable cause was satisfied in the case at hand, but not foreclosing a standard less than probable cause). *But see* Marks & Batey, *supra* note 134, at 1001 (criticizing such a standard in the context of electronic tracking devices as being too unrestrictive).

146 *See* Illinois v. Wardlow, 528 U.S. 119, 125 (2000) (holding that "reasonable suspicion must be based on commonsense judgments and inferences about human behavior").

147 *See* United States v. Karo, 468 U.S. 705, 718 n.5 (1984).

148 *Id.*

149 Some commentators have argued that despite the problems of the theory's application, the "mosaic theory" is nevertheless a viable theory in Fourth Amendment law. *See* Sanchez, *supra* note 11 ("Sorting all of this out going forward is likely to be every bit as big a headache as [Professor Kerr] suggests. But if the Fourth Amendment has a *point*—if it enjoins us to preserve a particular balance between state power and individual autonomy—then as technology changes, its rules of application may need to get more complicated to track that purpose, as they did when the Court ruled that an admirably simple property rule was no longer an adequate criterion for identifying a 'search.'").

statutorily-based.[150] Many pattern-detecting investigatory techniques—pen registers, trap and trace devices[151] and mail covers[152]—are regulated by federal statute, with the standard for issuance varying with respect to the perceived level of intrusiveness of the particular investigatory method. Other investigative techniques—such as the use of electronic tracking devices[153]—are relatively unregulated. To

150 If the "mosaic theory" does survive in the Fourth Amendment, statutory regulation must be provided to supplement the existing "mosaic theory" jurisprudence. Without such regulation, the theory will remain unworkable in application. *See supra* Part III.

151 The Electronic Communications Privacy Act regulates how law enforcement may utilize pen registers and trap and trace devices in criminal investigations. *See* 18 U.S.C. §§ 3121–3127 (2006 & Supp. III 2009). 18 U.S.C. § 3122(a) authorizes an attorney for the government or a state investigative or law enforcement officer to apply for an order to install and use a pen register or a trap and trace device. *See* 18 U.S.C. §3122(a) (2006). An application must include "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by [the applicant] agency." *Id.* § 3122(b)(2); *see also* 1 FISHMAN & MCKENNA, *supra* note 83, § 4:13 ("The most noteworthy aspect of § 3122(b)(2) is that it does not require a statement of facts establishing probable cause or reasonable suspicion to believe that the register or trap-and-trace device will produce 'information . . . likely to be relevant' to a criminal investigation. *All* that is required, by way of factual justification, is a certification to that effect." (alteration in original)). Upon application, a court shall issue the order if it finds that the applicant has made the requisite certification of relevancy. *See* 18 U.S.C. § 3123(a); *see also* S. REP. NO. 99-541, at 47 (1986) ("[§ 3123(a)] does not envision an independent judicial review of whether the application meets the relevance standard, rather the court needs only to review the completeness of the certification submitted."). The order authorizes the use of the pen register or a trap and trace device for a period not to exceed sixty days, although extensions may be granted. *See* 18 U.S.C. § 3123(c). Thus, the certification of relevancy required for the issuance of a pen register or a trap and trace device is far less stringent than a statement of facts establishing probable cause or reasonable suspicion.

152 *See* 39 C.F.R. § 233.3 (2010). Before the United States Postal Service can issue a mail cover order, the requesting law enforcement agency must specify, in a written request, "reasonable grounds to demonstrate the mail cover is necessary to: (i) Protect the national security, (ii) Locate a fugitive, (iii) Obtain information regarding the commission or attempted commission of a crime, or (iv) Assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law." *Id.* § 233.3(e)(2); *see also* 2 JOHN WESLEY HALL, JR., SEARCH AND SEIZURE § 29.7 (3d ed. 2000) ("Mail covers may still be used to investigate virtually any crime."). Thus, not only are mail cover orders issued to investigate a wide array of crimes, the standard to be met is lower than that required to obtain a warrant.

153 Unlike other types of investigatory techniques, electronic tracking devices are relatively unregulated. 18 U.S.C. § 3117(a) governs jurisdictional aspects of the use of tracking devices. *See* 18 U.S.C. § 3117(a). The statute provides that courts otherwise authorized to issue a warrant or other order for the installation of such a device can authorize the use of the device outside the court's own jurisdiction. *See id.* It does

protect privacy, Congress must enact legislative standards regulating both developing and existing unregulated pattern-detecting technologies.[154]

Some commentators have opined that protection against invasive technologies can be provided by legislative enactment.[155] Others argue that legislative protection is more of an "aspiration than reality,"[156] or contend that courts have a duty to protect invasions of privacy, and that legislative enactments should be supplementary to judicial efforts to provide protection.[157] Certainly the idea of Con-

---

not, however, require police to obtain court orders before installing or monitoring a tracking device nor provide law enforcement guidance in the use of the device. Rule 41(b)(4) of the Federal Rules of Criminal Procedure provides some guidance on the requirements for the issuance of a warrant for electronic tracking devices. *See* FED. R. CRIM. P. 41(b)(4). Pursuant to Rule 41, district magistrate judges have the authority to authorize the installation and use of electronic tracking devices to track an individual both within and outside of the district. *See id.* Upon application, a magistrate judge must issue the tracking warrant if there is probable cause. *See id.* R. 41(d)(1). A tracking device warrant must identify the target of the tracking and must specify a reasonable length of time that the device may be used, not exceeding forty-five days. *See id.* R. 41(e)(2)(C). This rule does not address whether law enforcement officers need a warrant to install or monitor a tracking device.

154 This Note does not suggest that Congress should be the sole protector of privacy against invasive technologies. Rather, courts should continue, and in fact have a duty to continue, analyzing the use of new and existing technologies in criminal investigations against the Fourth Amendment. What this Note suggests is that pattern-detecting technologies which have not been deemed searches in the first instance should be statutorily regulated to curb the potential deleterious effect on privacy from the continuous and prolonged use of such devices.

155 *See* 2 FISHMAN & MCKENNA, *supra* note 83, § 29:40 (recommending Congress enact legislation to regulate all aspects of tracking device surveillance by requiring law enforcement officials to obtain a court order based upon reasonable suspicion); Kerr, *supra* note 94, at 806 (contending that "the legislative branch rather than the judiciary should create the primary investigative rules when technology is changing").

156 Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 412 n.3 (2007).

157 *See* Blitz, *supra* note 107, at 1421 (recognizing arguments for a statutory solution to video surveillance, but concluding that courts "are not powerless to judge when the surveillance schemes involved in a particular dispute leave citizens with too little privacy"); Sherry F. Colb, *A World Without Privacy: Why Property Does Not Define the Limits of the Right Against Unreasonable Searches and Seizures*, 102 MICH. L. REV. 889, 903 (2004) ("Congress [may be] as good as or better than the courts at protecting privacy, but absent some reason to think that the courts will systematically overprotect privacy, the fact that we can generally rely upon the democratic process is no reason to forego the additional protection for individual rights that the judiciary affords for those occasions when majority rule threatens to become majority tyranny."); Slobogin, *supra* note 109, at 286–87 (arguing that courts should provide legislative bodies with a "constitutional road map" for the regulation of public surveillance); Peter P. Swire, Katz *Is Dead. Long Live* Katz., 102 MICH. L. REV. 904, 919 (2004) (contending that an

gress enacting legal standards that govern investigatory techniques in criminal investigations is not novel. Congress has, for instance, promulgated standards for the use of new technologies after the Supreme Court has ruled that they are a search within the meaning of the Fourth Amendment. For example, after the Court held in *Berger v. New York*[158] and *Katz*[159] that wiretapping and bugging fell within the ambit of the Fourth Amendment, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[160] which has since governed the interception of oral and wire communications.[161] Title III was significantly amended by Title I of the ECPA to include "electronic communications" to the types of communications protected from interception.[162] When a court assesses the constitutionality of the governmental use of such electronic surveillance, it often looks to the mandates of Title III and goes no further.[163]

Congress has also implemented standards for the use of certain technologies in criminal investigations after the Court has held such use to fall outside of the Fourth Amendment. After the Court in *Smith v. Maryland*[164] held that the installation and use of a pen register did not constitute a "search" within the meaning of the Fourth Amendment, Congress passed Title III of the ECPA, the Pen Register and Trap and Trace Devices Statute, which provided protection from the use of such devices.[165] Further, Congress has enacted regulation

---

approach where Congress took the primary responsibility for enacting privacy protections "would quite likely result in an impoverishment of the legislative debate about privacy and surveillance, and less effective deliberation on what safeguards are appropriate").

158 388 U.S. 41, 54–60 (1967) (holding that wiretapping under the New York wiretapping law did not satisfy the Fourth Amendment).

159 Katz v. United States, 389 U.S. 347, 353 (1967) ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

160 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211 (codified as amended at 18 U.S.C. §§ 2510–2522 (2006 & Supp. III 2009)).

161 *See supra* notes 135–139 and accompanying text.

162 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 101–111, 100 Stat. 1848, 1848–59 (codified as amended at 18 U.S.C. §§ 2510–2522).

163 *See* Kerr, *supra* note 94, at 850 ("When confronted with claims that wiretapping violated the Fourth Amendment, courts typically fall back on the statutory protections of Title III and go no further.").

164 442 U.S. 735, 745–46 (1979).

165 *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 301–303, 100 Stat. 1848, 1868–73 (codified as amended at 18 U.S.C.

aimed at invasive technologies that have yet to be addressed by the Court. For example, Title II of the ECPA, referred to as the Stored Communications Act, was enacted to regulate the storage of e-mails and Internet communications.[166] Even in the absence of statutorily mandated standards, rather than formulating Fourth Amendment standards, courts have adopted the statutory framework of other legislation.[167] Thus, in deciding the appropriate level of regulation for unregulated pattern-detecting technology in criminal investigations, Congress can look at its past body of work.

The implementation of legislative standards would be beneficial in several respects.[168] First, legislative standards would provide law enforcement with a workable set of investigatory standards. Provisions governing the issuance of court orders would provide law enforcement agents and judges clarity with respect to what information must be produced and what standard of review must be met. Any fear that subsequent monitoring would cross the mosaic threshold and render the entirety of an investigation unconstitutional would be eliminated. Second, abuses of investigatory techniques outside of the reach of the Fourth Amendment will be curbed—and privacy thus enhanced—by judicial review. Indiscriminate monitoring will be checked by the establishment of a standard of review for issuance and by providing a maximum period of permissible monitoring. Third, Congress has the flexibility to enact, amend, or repeal law until a proper balance is struck between individual privacy and police investigatory powers.[169]

---

§§ 3121–3127); *see also supra* note 151 and accompanying text (discussing the statutory regulation of law enforcement use of pen registers and trap and trace devices in criminal investigations).

166 *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 201–202, 100 Stat. 1848, 1860–68 (codified as amended at 18 U.S.C. §§ 2701–2712).

167 *See supra* notes 142–44 and accompanying text.

168 *See* 2 FISHMAN & MCKENNA, *supra* note 83, § 29:40 (noting benefits of the implementation of electronic tracking legislation to be (1) "enhancing individual privacy and providing a check against potential abuse" by providing judicial review; (2) "enhanc[ing] effective law enforcement" by providing clarity in the law; and (3) "establish[ing] standardized procedures governing the issuance and execution of such court orders"); Kerr, *supra* note 94, at 859 ("The context of legislative rule-creation offers significantly better prospects for the generation of balanced, nuanced, and effective investigative rules involving new technologies.").

169 *See* Kerr, *supra* note 94, at 871 ("Legislatures can experiment with different rules and make frequent amendments; they can place restrictions on both public and private actors; and they can even 'sunset' rules so that they apply only for a particular period of time. The courts cannot. As a result, Fourth Amendment rules will tend to lack the flexibility that a regulatory response to new technologies may require." (footnotes omitted)).

It is one thing to say that the legislature, rather than the Court, should be charged with providing standards governing the use of pattern-detecting investigatory techniques in criminal investigations, and quite another to define precisely what the appropriate standard should be. Certainly some level of particularized suspicion is necessary.[170] The precise amount, however, should reflect the intrusiveness of the investigatory method. One possibility is an amendment for the inclusion of pattern-detecting technologies in Title III. Such an amendment, however, is only appropriate if the technology is of such an intrusive and indiscriminate nature as to warrant the heightened requirements of Title III. Here, it is not likely that location patterns are of such an intrusive and indiscriminate nature as to render Title III applicable. As for indiscriminateness, the use of location patterns is just as indiscriminate as wiretapping, bugging, or even video surveillance. That is, electronic tracking will pick up all locations within electronic reach, without regard to the relevance of the location to the investigation. Unlike wiretapping, bugging, or video surveillance, the use of pattern-detecting technologies is not more invasive of privacy.[171] Surely a video of an individual walking into a particular building or the interception of the conversation that ensued while the individual was at the location is more invasive than the physical coordinates of such location. Not only do the devices not pick up sounds or video, the geographical coordinates will not in and of themselves confirm that a particular individual was at each particular place within the pattern. The coordinates do not reveal who was in the vehicle, what was happening or what was said in the vehicle, or whether an individual in fact exited the vehicle to visit a specific location. What this analysis suggests is that while the use of electronic tracking devices to intercept digital location patterns may be just as indiscriminate as traditional forms of surveillance covered by Title III, it is much less invasive and thus should not be subject to Title III's restrictive requirements.

Moreover, if location pattern-detecting technology was so indiscriminate and invasive to warrant the application of Title III requirements, Title III would provide overbroad protection. The requirements of Title III extend only to "oral communications" in

170 *See* Solove, *supra* note 15, at 1109 ("Particularized suspicion keeps the government's profound investigative powers in check preventing widespread surveillance and snooping into the lives and affairs of all citizens.").

171 *See* 2 FISHMAN & MCKENNA, *supra* note 83, § 29:26 (noting that electronic tracking is far less intrusive than other investigatory techniques, such as wiretapping and eavesdropping).

which individuals have a justifiable expectation of non-interception.[172] This limitation, however, is absent in the definition of both wire and electronic communications.[173] As pattern-detecting technology would fall under wire or electronic communication, the communication is protected from unauthorized interception even if the participants do not have a justifiable expectation of non-interception.[174] Accordingly, Title III would treat all types of pattern information as protected, regardless of whether such information would be deserving of protection under the Fourth Amendment. Thus, a higher standard than probable cause is not appropriate for location pattern-detecting technologies.[175]

The conclusion that the heightened requirements of Title III are not appropriate for pattern-detecting technologies leaves Congress with alternatives such as probable cause, reasonable suspicion, or a statement of relevance. The question of the precise level of protection should be left to Congress—a body with the institutional capacity and experience to make such a decision.

CONCLUSION

The use of emerging and existing intrusive technologies in criminal investigations certainly has the potential to have a substantial effect on privacy. In an effort to combat the threat of such use, *Maynard* introduced the "mosaic theory" into Fourth Amendment law. The "mosaic theory" holds that individual law enforcement acts that are not "searches" become a "search" when aggregated, as the whole reveals more than the individual acts it comprises. This Note suggests that despite the intuitive appeal of a "mosaic theory," the use of the

172 *See* 18 U.S.C. § 2510(2) (2006); *see also* 1 FISHMAN & MCKENNA, *supra* note 83, § 2.24 (describing concept as the "expectation of non-interception").

173 *See* 18 U.S.C. § 2510(1); *id.* § 2510(12).

174 *See* Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 WASH. & LEE L. REV. 1287, 1300 (2000) (criticizing the justifiable expectation of non-interception language in the context of internet communications as it would cover not only private internet communications, but also "[w]eb pages in transit, commands sent to remote servers, picture or music files, network support traffic, and almost everything else in cyberspace"); Simmons, *supra* note 34, at 1340–41 ("In this sense, statutory protection for electronic communications is too broad, treating all internet traffic as deserving of an equal amount of protection and thus forcing government agents to acquire a Title III order for even the most mundane transmissions that would not deserve privacy under the *Katz* test.").

175 *See* 1 LAFAVE, *supra* note 20, § 2.7(e) (rejecting a higher standard than probable cause with respect to location monitoring as "[a]scertaining the location of an object on a continuing basis falls far short of the repeated interception of private conversations").

theory in Fourth Amendment law is misguided. The "mosaic theory" is inconsistent with the Supreme Court's voluntary exposure analysis, which has often classified theoretical or limited disclosures of information as complete exposures warranting no Fourth Amendment protection.[176] It is also inconsistent with the Supreme Court's implicit rejection of the proposition that the Fourth Amendment analysis is altered when an investigatory technique is prolonged to the point where information may be accumulated.[177]

Not only is the theory inconsistent with existing Fourth Amendment jurisprudence, it is also impractical in application. A problematic question arises as to what durational threshold must be crossed in order for the use of a pattern-detecting technology to be sufficiently prolonged as to render it a search. Once this illusive threshold is crossed and a mosaic is created, the question that then arises is how to define the scope of the mosaic. If a pattern is created only through the use of multiple investigatory techniques, the entire investigation will be rendered a search. Also left unanswered is the appropriate standard of review for the use of pattern-detecting investigatory techniques in criminal investigations. The most serious implication of the theory, however, is that it calls into question a number of previously accepted investigatory techniques.

The "mosaic theory," if applied consistently, would revolutionize the Fourth Amendment and how criminal investigations are conducted. Such a revolutionary response to pattern-detecting technologies and investigative techniques is hardly the type of judicial restraint recently urged by the Supreme Court in *City of Ontario v. Quon*.[178] Rather than regulating pattern-detecting techniques constitutionally at the aggregate level, privacy interests should be statutorily protected.

176 *See supra* note 83.

177 *See supra* note 89–92 and accompanying text.

178 130 S. Ct. 2619, 2629 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." (citing Olmstead v. United States, 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347, 353 (1967), *and* Berger v. New York, 388 U.S. 41 (1967))).