Tennessee Law Review

Volume 82
Issue 4 *Summer 2015*

Article 6

2015

TRANQUILITY & MOSAICS IN THE FOURTH AMENDMENT: HOW OUR COLLECTIVE INTEREST IN CONSTITUTIONAL TRANQUILITY RENDERS DATA DRAGNETS LIKE THE NSA'S TELEPHONY METADATA PROGRAM A SEARCH

Michael Gentithes

TRANQUILITY & MOSAICS IN THE FOURTH AMENDMENT: HOW OUR COLLECTIVE INTEREST IN CONSTITUTIONAL TRANQUILITY RENDERS DATA DRAGNETS LIKE THE NSA'S TELEPHONY METADATA PROGRAM A SEARCH

MICHAEL GENTITHES*

INTRODUCTION

In the Fourth Amendment struggle to balance liberty and security, the third-party doctrine in *Smith v. Maryland*, as applied to telephonic communications, has long held sway.[1] For more than thirty years, government investigators have relied on *Smith* when accessing, without a warrant, information citizens have voluntarily disclosed to third parties.[2] The government has also assumed that *Smith* controls the analysis of far-reaching "data dragnets,"[3] like the

---

* LL.M, New York University School of Law, 2011; J.D., DePaul University College of Law, 2008; B.A. Colgate University 2005. I am extremely grateful for the helpful comments of Laura K. Donohoe, Geoffrey Stone, Barry Friedman, Stephen Siegel, and Matthew Lawrence.

1. Smith v. Maryland, 442 U.S. 735 (1979).

2. *See, e.g.*, Hanni Fakhoury, Smith v. Maryland *Turns 35, but its Health is Declining*, ELECTRONIC FRONTIER FOUND. (June 24, 2014), https://www.eff.org/deeplinks/2014/06/smith-v-maryland-turns-35-its-healths-declining (explaining the "third-party doctrine" and how the government uses it to justify electronic surveillance).

3. I use this term throughout the article to refer to programs utilizing modern technology to harvest information available about users of modern computing and communication technology. That relatively accessible information is sometimes

National Security Agency's ("NSA") recently revealed program for the collection of telephony metadata.[4] This assumption goes too far. While *Smith*'s thirty-six-year-old reasoning remains applicable to the facts of that case, the decision does not resolve modern constitutional quandaries presented by the government's capability to collect and aggregate massive amounts of civilian information.

In this article, I consider alternatives to the *Smith* analysis that might explain why the NSA's program, and others like it, rise to the level of a search, implicating Fourth Amendment interests. I begin with a discussion of the strengths—and one especially glaring weakness—of the so-called "mosaic theory" of the Fourth Amendment.[5] The theory suggests that the government's use of modern data dragnets might constitute a search, even if no citizen has a privacy interest in the individual data points collected, because, at some level, constant and ubiquitous monitoring paints such a detailed "mosaic" of one's life that it triggers Fourth Amendment protection.[6] The quantitative whole of all the data

---

referred to as "big data." *See, e.g.*, *Data, Data Everywhere*, ECONOMIST (Feb. 25, 2010), http://www.economist.com/node/15557443.

4. *See* Glen Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 5, 2013, 6:05 AM), www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

5. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012) (explaining the origins of the "mosaic theory" in Fourth Amendment doctrine).

6. "The fundamental insight behind the mosaic theory is that we can maintain reasonable expectations of Fourth Amendment privacy in certain quantities of information and data even if we lack reasonable expectations of privacy in the constituent parts of that whole." David Gray & Danielle K. Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 390 (2013) [hereinafter Gray & Citron, *A Shattered Looking Glass*]; *see also* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 68-69 (2013) [hereinafter Gray & Citron, *Quantitative Privacy*]. Traces of this theory are found throughout Justice Alito's concurrence in *United States v. Jones*, 132 S. Ct. 945, 957-64 (2012), which concerned long-term police monitoring through the use of a GPS device. Justice Alito reasoned that:

> The critical distinction . . . was that, for practical reasons, the police cannot physically "monitor and catalogue every single movement of an individual's car for a very long period." The traditional form of surveillance—following the person—is realistic only in extraordinary circumstances. . . . The advent of GPS, however, has changed the situation dramatically, and individuals, he concluded, do have a reasonable expectation of privacy that the police will not use this new technology without restraint to track their every move.

collected provides too clear a picture of the subject's existence to be called a non-search.[7] The mosaic theory, while promising, includes a logical inconsistency with no apparent solution; it claims that some undefined quantity of non-searches amount to a search, and thus commits quantitative error for which no effective rejoinder has yet been proposed.[8]

But another interest is implicated by data dragnets as broad as the NSA's, one which explains why those programs should meet the strictures of the Fourth Amendment—a collective Fourth Amendment interest is shared by all citizens utilizing telecom services, one that is infringed upon by the NSA's data collection program. But such a group interest cannot be based on notions of personal privacy alone. Instead, millions of Americans share a joint Fourth Amendment interest in constitutional tranquility, an interest woven throughout the Constitution,[9] that is implied in Justice Brandeis's expression of the Fourth Amendment's primary aim—to protect citizens' "right to be let alone."[10] Constitutional tranquility implies citizens' freedom from undue government harassment, even if, in intruding upon it, the government never accesses anything truly "private," and keeps its activities entirely covert. While the accumulation of millions of non-invasions of privacy cannot amount to one large invasion of privacy, each individual government action

---

Geoffrey R. Stone, *Is the NSA's Bulk Telephony Meta-Data Program Constitutional: PART II*, HUFFINGTON POST (Jan. 6, 2014, 12:12 PM), www.huffingtonpost.com/geoffrey-r-stone/is-the-nsas-bulk-telephon_b_4549449.html.

7. Under this theory then, "[i]dentifying Fourth Amendment searches requires analyzing police actions over time as a collective 'mosaic' of surveillance; the mosaic can count as a collective Fourth Amendment search even though the individual steps taken in isolation do not." Kerr, *supra* note 5, at 313.

8. Phrased differently, if the government only seeks information "not otherwise worthy of the protection [of the Fourth Amendment], it seems no justification for requiring probable cause to say that 'we know you *could* acquire so much third-party information from existing records that we are going to require a warrant even for this minimal request.'" Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 1023 (2007) (citation omitted). This issue was also noted by the D.C. Circuit in the *Jones* case: "[t]he 'sum of an infinite number of zero-value parts is also zero.'" Gray & Citron, *A Shattered Looking Glass*, *supra* note 6, at 399 (quoting United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, J., dissenting)).

9. *See generally* U.S. CONST. pmbl. ("We the people of the United States, in Order to form a more perfect Union, establish Justice, *insure domestic Tranquility* . . . .") (emphasis added).

10. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

does constitute a greater-than-zero infringement upon constitutional tranquility, and the aggregate of those actions may constitute a search.

In the final portions of the article, I suggest that opponents of data dragnets should rely on the collective interest in constitutional tranquility to distinguish *Smith*, rather than argue for its direct overrule. In light of the Supreme Court's most elaborate statements on the *stare decisis* doctrine, *Smith* is a precedent that should be maintained.[11] Although *Smith*'s age might give the Court pause in applying it to data dragnets, the opening it provides should be utilized to argue for a mosaic theory enhanced by constitutional tranquility interests, not a reversal of one of the pillars of Fourth Amendment jurisprudence.

In short, Part I provides a brief history of the third-party doctrine in Fourth Amendment jurisprudence, demonstrating how it evolved into a mainstay of the Supreme Court's interpretation of a search.[12] Part II provides an example of a data dragnet that government agents justified using the third-party doctrine—the NSA's telephony metadata program.[13] Next, Part III considers the strength of the mosaic theory for distinguishing the government's actions in *Smith* from its actions in modern data dragnets.[14] Finding that theory wanting, Part IV details citizens' shared interest in constitutional tranquility, explaining how that interest can provide the intellectual support needed for its integration into modern Fourth Amendment jurisprudence.[15] Finally, Part V suggests that opponents of data dragnets should favor the mosaic theory augmented by constitutional tranquility over efforts to overturn the *Smith* decision.[16]

---

11. *See, e.g.*, Vasquez v. Hillery, 474 U.S. 254, 265 (1986) (describing *stare decisis* as "the means by which we ensure that the law will not merely change erratically, but will develop in a principled and intelligible fashion"). The Court further highlights the importance of *stare decisis*, stating that it "permits society to presume that bedrock principles are founded in the law rather than in the proclivities of individuals, and thereby contributes to the integrity of our constitutional system of government, both in appearance and in fact." *Id.* at 265-66.

12. *See infra* Part I.

13. *See infra* Part II.

14. *See infra* Part III.

15. *See infra* Part IV.

16. *See infra* Part V.

I. A BRIEF HISTORY OF THE THIRD-PARTY DOCTRINE

The Fourth Amendment to the United States Constitution provides that:

> 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]

One of the greatest difficulties in applying this text is determining which government activities constitute "searches and seizures." Answering that question has led the Court down a number of unexpected jurisprudential paths, including the third-party doctrine discussed in this article.[18] A brief history of the Court's evolving definition of a "search" provides useful background on the doctrine's evolution.

In early cases grappling with the scope of the term "search," the Supreme Court focused on the amendment's relationship to "common-law trespass, at least until the latter half of the 20th century."[19] Cases such as *Olmstead v. United States* exemplified this trend, holding that taps attached to telephone wires in public streets did not run afoul of the Fourth Amendment because the government had not intruded upon any of the material things mentioned in the amendment—a citizen's person, house, papers, or effects.[20] But *Olmstead* also presaged a shift in the direction of Fourth Amendment jurisprudence. In his dissent, Justice Brandeis expounded upon the Amendment's core values, describing its grounding in "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[21] Brandeis emphasized the measures the framers undertook to ensure that this treasured right was not trampled by government investigations,

---

17. U.S. CONST. amend. IV.

18. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) (identifying the "third-party consensual surveillance cases," which laid the groundwork for the third-party doctrine).

19. United States v. Jones, 132 S. Ct. 945, 949-50 (2012) (citations omitted).

20. Olmstead v. United States, 277 U.S. 438, 463-64 (1928).

21. *Id.* at 478 (Brandeis, J., dissenting). Since *Olmstead*, Justice Brandeis's words have been quoting many times. *See, e.g.*, Scott E. Sundby, *"Everyman" 's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1755-56 (1994) (highlighting the importance of the Fourth Amendment's founding principles).

arguing that "[t]o protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[22]

Brandeis's argument slowly gained traction, and *Katz v. United States* formalized it nearly forty years later.[23] *Katz* concerned an eavesdropping device attached to a public telephone booth.[24] In *Katz*, the Court emphasized that "the Fourth Amendment protects people, not places."[25] In an oft-cited concurrence, Justice Harlan suggested that government conduct amounts to a search, triggering Fourth Amendment protection, when it intrudes upon a citizen's "constitutionally protected reasonable expectation of privacy."[26] Justice Harlan argued that in order for a citizen to demonstrate governmental intrusion upon such a reasonable expectation of privacy, she must meet "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.'"[27] While recent decisions have re-emphasized that the Fourth Amendment "embod[ies] a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates,"[28] the reasonable expectation of privacy test has become the touchstone for determining whether government conduct constitutes a Fourth Amendment search.[29]

Critics suggest that Harlan's twofold test in *Katz* constitutionalizes the subjective attitudes of Supreme Court Justices.[30] If Justices interpreted the *Katz* test literally, "a sense of how (innocent) U.S. citizens gauge the impact of police investigative

---

22. *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting).

23. Katz v. United States, 389 U.S. 347, 350-51 (1967).

24. *Id.* at 348.

25. *Id.* at 351.

26. *Id.* at 360 (Harlan, J., concurring).

27. *Id.* at 361.

28. United States v. Jones, 132 S. Ct. 945, 950 (2012).

29. *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 211 (1986) (citing Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)) (describing "reasonable expectation of privacy" as the "touchstone of Fourth Amendment analysis").

30. *See* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1512 n.5 (2010) (citing Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1321 (1981); Sherry F. Colb, *What is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002); Richard G. Wilkins, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077, 1080 (1987)).

techniques on their privacy and autonomy," perhaps derived from thorough social science research and polling data, would be "highly relevant to current Fourth Amendment jurisprudence."[31] Yet the Court has long resisted this kind of empirical approach to the definition of a search, and for good reason. While relying upon the Justices' collective sense of societal expectations is a less-than-ideal manner to determine the Fourth Amendment's scope, it is practically impossible to avoid.

As professor Daniel Solove notes, "[f]ollowing surveys would make the Fourth Amendment too shackled to the preferences of the majority. Moreover, it would strike many as illegitimate because the Constitution is supposed to transcend the will of the majority at any particular moment in time."[32] Furthermore, as members of the Court have noted, government agents might influence popular perceptions of privacy by announcing their plans to invade certain realms previously regarded as private.[33] It would be self-defeating to the let the government define the scope of a constitutional rule designed to prohibit against government overreach. As a general matter, it seems that the determination of whether a particular action constitutes a search may be best left to somewhat speculative judicial determinations. Over time, though, that approach has produced outcomes of dubious normative value, such as the third-party doctrine.[34]

Under the third-party doctrine, a citizen uniformly relinquishes any expectation of privacy in information disclosed to a third party.[35] As the Supreme Court has summarized:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[36]

---

31. Cristopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 732 (1993).

32. Solove, *supra* note 30, at 1522.

33. *See* Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting) (noting the possible influence of government agents).

34. *See* United States v. Miller, 425 U.S. 435, 443 (1976) (explaining the constitutional rationale for the third-party doctrine).

35. *See id.*

36. *Id.*

The doctrine thus provides a simple, bright-line rule: Government collection of such third-party information, no matter how intrusive, does not constitute a search subject to Fourth Amendment requirements.[37]

The third-party doctrine first emerged in cases concerning verbal statements made to third-party government informants—situations where "the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications."[38] However, that straightforward version of the doctrine has grown through decades of decisions. Many of those expansions, including the ones described below, have been subject to widespread scholarly criticism.[39]

In *United States v. Miller*, government investigators obtained financial records from the defendant's bank via an allegedly defective subpoena.[40] The defendant challenged the admission of his bank records on the grounds that they were the product of an unlawful search.[41] Consequently, the Supreme Court chose to expand the third-party doctrine to include records such as those disclosed by the bank.[42] The Court held that because "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business,"

---

37. *See id.*

38. *Smith*, 442 U.S. at 749 (1979) (Marshall, J., dissenting) (citing United States v. White, 401 U.S. 745, 751-52 (1971); Hoffa v. United States, 385 U.S. 293, 302-03 (1966); Lopez v. United States, 373 U.S. 427, 439 (1963)).

39. For a summation of such critiques, see Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 n.5 (2009) (citing CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 151-64 (2007); Ashdown, *supra* note 30, at 1315; Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211 (2006); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3; Henderson, *supra* note 8, at 975; Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L. J. 549, 564-66 (1990); Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & TECH. 2, 3-4; Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229 (1983); Sundby, *supra* note 21, at 1757-58; Andrew J. DeFilippis, Note, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1092 (2006)).

40. United States v. Miller, 425 U.S. 435, 436 (1976).

41. *Id.*

42. *Id.* at 442.

there was no reasonable expectation of privacy in those records.[43] "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[44] The depositor's assumption of risk was tantamount to her consent, allowing the bank to disclose her records.[45] The government's warrantless collection of bank information in *Miller*, therefore, did not amount to a search, and the Fourth Amendment was not implicated.[46]

The *Miller* Court's interpretation of the third-party doctrine provided the intellectual basis for its widely-criticized decision in *Smith v. Maryland*.[47] In *Smith*, police officers requested that a telephone company install a pen register in its central offices to record the numbers dialed from the defendant's home phone.[48] The pen register disclosed only the telephone numbers that the defendant dialed; it did not reveal the contents of the communication, the reason for the call, the identity of the parties, or whether the call was completed.[49] The police, however, did not obtain a warrant or a court order before requesting the pen register's installation.[50]

When the defendant challenged the introduction of evidence collected via pen register, the Court held that the device's installation did not constitute a search under the Fourth Amendment because the defendant had no reasonable expectation of privacy in the numbers he dialed.[51] Relying on the *Miller* Court's reasoning that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," the *Smith* Court held that telephone users have no expectation of privacy in the numbers that they disclose to a telephone company when placing a

---

43. *Id.*

44. *Id.* at 443.

45. Another rationale underlying the Court's decision in *Miller* was the fact that banks traditionally kept these records, so the government's effort to collect them was not a "novel means designed to circumvent established Fourth Amendment rights." *Id.* at 444. The NSA's dragnet program for the collection of telephonic metadata is arguably just that kind of novel circumvention, as the third-party phone companies involved did not traditionally keep the information the government sought through its dragnet program until receiving instruction to do so via court order. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 36 n. 57 (D.D.C. 2013).

46. *Miller*, 425 U.S. at 442.

47. Smith v. Maryland, 442 U.S. 735 (1979).

48. *Id.* at 737. In *Smith*, the police began surveilling the defendant after he was suspected of robbing, and later harassing, a Baltimore woman. *Id.*

49. *Id.* at 741.

50. *Id.* at 737.

51. *Id.* at 742-46.

call.[52] Indeed, telephone users "typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[53] Thus, the Court concluded that the government was not required to obtain a warrant prior to collecting information through a pen register because the defendant had no reasonable expectation of privacy in that information.[54]

Critiques of *Smith* have been wide and varied, even coming from some of the Justices themselves.[55] In his dissent, Justice Stewart questioned the majority opinion's affirmation that telephone users know or expect that the government might utilize a pen register.[56] According to Stewart, it was "simply not enough to say, after *Katz*, that there is no legitimate expectation of privacy in the numbers dialed because the caller assumes the risk that the telephone company will disclose them to the police."[57]

Justice Marshall's vigorous dissent even more pointedly dissected the majority's assumption of the risk rationale.[58] Justice Marshall noted that:

> Implicit in the concept of assumption of risk is some notion of choice. . . . By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.[59]

Justice Marshall also pointed out the dramatic chilling effect this type of government monitoring could have on otherwise constitutionally protected activities.[60] He noted that "[p]rivacy in placing calls is of value not only to those engaged in criminal activity. The prospect of unregulated governmental monitoring will

---

52. *Id.* at 743-45 (citing United States v. Miller, 425 U.S. 435, 442-44 (1976)).

53. *Smith*, 442 U.S. at 743.

54. *Id.* at 745-46.

55. *See, e.g.*, *id.* at 746-48 (Stewart, J., dissenting) (criticizing the majority's opinion in *Smith*, noting that the general public would not know, or even understand, that phone companies use devices such as pen registers).

56. *Id.*

57. *Id.* at 747 (Stewart, J., dissenting).

58. *See id.* at 749-50 (Marshall, J., dissenting).

59. *Id.* (citations omitted).

60. *See id.* at 751.

undoubtedly prove disturbing even to those with nothing illicit to hide."[61]

As critiques of *Smith* have intensified, some Supreme Court Justices have expressed a desire to revisit its holding.[62] In *United States v. Jones*, which concerned the use of a GPS tracking device attached to the defendant's car, Justice Sotomayor candidly discussed the ill-fit between the third-party doctrine of old, and cases involving today's data dragnets.[63] Justice Sotomayor noted that:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.[64]

Though her critiques are based on a subjective view of what the public reasonably expects to remain private, her logical critique resonates with modern consumers of cellular and web-based technology. Justice Sotomayor, quite plausibly,

> [D]oubt[ed] that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year .... [She] would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[65]

---

61. *Id.*

62. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (criticizing the third-party doctrine's application to modern data dragnets).

63. *Id.*

64. *Id.* (citing Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 443 (1976)).

65. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring). There is an important counter-current regarding reasonable expectations of privacy in emerging technologies: As new communication devices play greater roles in our daily lives, we become more vulnerable to attack from outside parties, and thus the expectation of privacy in that information may shrink. As Scott Sundby put it:

> [B]ecause the Court is not asking whether bank or phone records *should* be kept private (thus invoking privacy as a value), but, rather, whether we as a *factual* matter expect others to see and use those records (thus viewing

Some commentators, such as Orin Kerr, have responded with valiant efforts to defend the third-party doctrine.[66] Kerr argues that the third-party doctrine preserves a needed societal balance between criminals and government investigators.[67] Crimes occur, at least partially, in public places open to government search, but a criminal's use of third parties threatens to upset that balance by "tak[ing] open and public portions of crimes and hid[ing] them from public observation."[68] Thus, government investigators must have access to information disclosed to third parties to restore the public-private balance in illicit activities.[69]

Kerr also suggests that "[d]isclosure to third parties eliminates protection [under the Fourth Amendment] because it implies consent."[70] "Third-party disclosure eliminates privacy because the target voluntarily consents to the disclosure, not because the target's use of a third party waives a reasonable expectation of privacy."[71] This seems a fair recapitulation, persuasive or not, of the "assumption of the risk" idea at the heart of the *Smith* decision.[72]

> privacy as a measurable fact), Fourth Amendment protections will shrink as our everyday expectations of privacy also diminish.

Sundby, *supra* note 21, at 1760-61 (alteration in original) (citations omitted); *see also* Brenner & Clarke, *supra* note 39, at 219 ("More than ever before, the details about our lives are no longer our own. They belong to the companies that collect them, and the government agencies that buy or demand them in the name of keeping us safe.").

66. *See generally* Kerr, *supra* note 39, at 563-66 (justifying the government's use of the third-party doctrine to apprehend criminals).

67. *Id.* at 573-76.

68. *Id.* at 564.

69. *Id.* at 575-76. "Without the third-party doctrine, savvy wrongdoers could use third-party services in a tactical way to enshroud the entirety of their crimes in zones of Fourth Amendment protection." *Id.* at 564. While slightly beyond the scope of this article, one might retort to Kerr's defense of the balancing role of the third-party doctrine that he assumes the guilt of the parties being investigated, or at least the vast majority of those that the government trains its resources on. But the relevant question is what the Fourth Amendment allows the government to access freely regarding the innocent. When the issue is phrased that way, the doctrine appears far more overreaching.

70. *Id.* at 565. The third-party doctrine is thus a "subset of consent law." *Id.*

71. *Id.* at 588. Kerr adds that "[s]o long as a person knows that they are disclosing information to a third party, their choice to do so is voluntary and the consent valid." *Id.*

72. *Id.* at 564. "The fact that a person turns out to be an undercover agent should be irrelevant to whether the consent is valid, as that representation is merely fraud in the inducement rather than fraud in the factum." *Id.* at 588.

II. THE NSA'S TELEPHONY METADATA COLLECTION PROGRAM

While it may have fallen into some disfavor, *Smith* remains, for the law enforcement community, a fixture of Fourth Amendment jurisprudence. It is likewise at the heart of recent efforts by the NSA to collect cellular telephone metadata—the characteristics, but not the content, of cellular communications—through an enormous dragnet program revealed through "leaks" of information obtained by former NSA employee Edward Snowden.[73] While this article addresses the Fourth Amendment implications of all data dragnets, it is worthwhile to briefly detail the NSA's program, at least as it stood prior to modifications enacted in summer 2015,[74] as an example that provides context for later theoretical discussion.[75]

The NSA's telephony metadata collection program is the product of a series of congressional and judicial authorizations as well as the evolving technological capabilities of the agency.[76] The program draws its authority from the Foreign Intelligence Surveillance Act ("FISA"), passed in 1978 and amended by the Patriot Act in 2001.[77] FISA established the Foreign Intelligence Surveillance Court

---

73. *See* Greenwald, *supra* note 4 (explaining the NSA's bulk data collection program).

74. *See* Jennifer Steinbauer & Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 Is Sharply Limited*, N.Y. TIMES (June 2, 2015), http://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=1 (describing the sweeping Congressional cutbacks made to government surveillance programs).

75. Evidence suggests that the public perceives the NSA's program as overly intrusive, even in the name of defending against terrorist threats. *See* Glen Greenwald, *Major Opinion Shifts, in the US and Congress, on NSA Surveillance and Privacy*, GUARDIAN (July 29, 2013), www.theguardian.com/commentisfree/2013/jul/29/poll-nsa-surveillance-privacy-pew. Indeed:

> Among other things, Pew finds that "a majority of Americans—56%—say that federal courts fail to provide adequate limits on the telephone and internet data the government is collecting as part of its anti-terrorism efforts." And "an even larger percentage (70%) believes that the government uses this data for purposes other than investigating terrorism." Moreover, "63% think the government is also gathering information about the content of communications."

Id.

76. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 11-12 (D.D.C. 2013) (describing the origins of the collection program).

77. *Id.*

("FISC"), composed of eleven district court judges, appointed by the Chief Justice of the Supreme Court.[78] FISC hears government applications for orders authorizing domestic electronic surveillance upon a showing that the target is a foreign power, or an agent of a foreign power.[79]

When Congress passed the Patriot Act, following the September 11th attacks, it added section 215 to FISA, extending the government's subpoena power to foreign intelligence investigations, with the added twist that such orders would remain secret.[80] In May 2006, FISC began issuing orders directing certain telecommunications companies to produce to the NSA, on an ongoing daily basis, telephony metadata records those companies create when providing communications services to their customers.[81] This includes the records of millions of American citizens, "none of whom are themselves suspected of anything."[82] The NSA then consolidates

---

78. *Id.* at 12 n.13.

79. *Id.*

80. *Id.* at 12-13. Specifically, it allowed the government to obtain orders from FISC directing individuals and third parties to disclose any number of "tangible things" upon a showing that the government has "reasonable grounds to believe" that the things sought are "relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(b)(2)(A); *see also* Geoffrey R. Stone, *The NSA's Telephone Meta-data Program: Part I*, HUFFINGTON POST (Dec. 24, 2013, 8:42 PM), www.huffingtonpost.com/geoffrey-r-stone/nsa-meta-data_b_4499934.html. Amendments to the Patriot Act in 2006 created a procedure through which a recipient of a FISC production order—and only the recipient of that order—can seek judicial review before the FISC review pool judges. *Klayman*, 957 F. Supp. 2d at 13-14. Due to the sensitive intelligence matters involved, FISC grants orders without adversarial testing of the government's claim that it has reasonable grounds to believe the information it seeks is relevant to an authorized investigation. *Id.* This is why the President's Independent Review Group on Intelligence and Communications Technologies recommended establishing a public advocate to represent privacy concerns in front of FISC, a recommendation that President Obama subsequently endorsed. *See* Peter Baker & Charlie Savage, *Obama to Place Some Restraints on Surveillance*, N.Y. TIMES (Jan. 14, 2014), http://www.nytimes.com/2014/01/15/us/politics/judge-warns-proposed-safeguards-could-hamper-surveillance-court.html?_r=0. Lack of public advocates illustrates the potential for government overreach when a new surveillance technology emerges.

81. *See Klayman*, 957 F. Supp. 2d at 16; Greenwald, *supra* note 4; Stone, *supra* note 80. Though this information does not include the contents of any conversations, it does include "the numbers of both parties on a call . . . location data, call duration, unique identifiers, and the time and duration of all calls." Greenwald, *supra* note 4.

82. Stone, *supra* note 80.

those metadata records into a singular database, where the FISC order permits it to retain the records for up to five years.[83]

These records do not include any information regarding the content of calls between users.[84] They do, however, include significantly more information than was collected by the pen register considered in *Smith*.[85] That device simply "recorded numbers on a paper tape, and did not even reveal whether the call went through, let alone how long it lasted."[86] The NSA's metadata program, in contrast, includes information about whether the call was completed, the call's duration, and possibly even the user's location.[87]

As noted earlier, the NSA may preserve and retain these records for up to five years, rather than merely a few days or through the course of a single investigation.[88] As long as the FISC orders remain in place, the collection of this data could continue indefinitely.[89] The NSA has thus obtained a vast database that may be accessed again and again on a potentially infinite timeline.[90]

FISC's orders do, however, place extensive restrictions upon the NSA's legal access to the telephony metadata database.[91] For an NSA employee to perform a "query" on the database, she must gain approval from one of twenty-two designated high-ranking officials within the NSA.[92] Those officials may grant approval only after determining that "there exist facts giving rise to a reasonable,

---

83. *See Klayman*, 957 F. Supp. 2d at 16; Stone, *supra* note 80.

84. Stone, *supra* note 80.

85. *See generally* Smith v. Maryland, 442 U.S. 735, 741 (1979) (describing the information gathered by the pen register).

86. Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 71 (2004).

87. *Klayman*, 957 F. Supp. 2d at 35-36 n.57.

88. *Id.* at 15.

89. *See id.* at 32. "[T]here is the very real prospect that the program will go on for as long as America is combating terrorism, which realistically could be forever!" *Id.*

90. Although recent reports suggest that the NSA has collected telephony metadata on only a subset of all domestic phone calls, that is still a substantial number. Charlie Savage, *N.S.A. Program Gathers Data on a Third of Nation's Calls, Officials Say*, N.Y. TIMES (Feb. 7, 2014), http://www.nytimes.com/2014/02/08/us/ politics/nsa-program-gathers-data-on-a-third-of-nations-calls-officials-say.html?_r=0. While those reports identify technical hurdles facing the NSA's efforts to collect metadata, the program's administrators aim to overcome those hurdles and obtain all domestic telephony metadata for the database. *Id.* (noting that officials "did not want to draw attention to the gap and because it is, in fact, the agency's goal to overcome technical hurdles that stop them from ingesting" data regarding all domestic calls).

91. *Klayman*, 957 F. Supp. 2d at 15-16.

92. *Id.* at 16.

articulable suspicion . . . that the selection term to be queried is associated with one or more of the specified foreign terrorist organizations approved for targeting by the FISC."[93]

In 2012, only 288 queries were approved through this procedure.[94] Furthermore, a query's results are limited only to those numbers *previously associated with terrorism* that called, or were called by, the "seed" number of the query.[95] These immediate contacts are known as the "first hop" of contacts from the seed number.[96] The NSA is permitted to make a second "hop," meaning it can use the database to determine if any of those first-order connections to the seed number called, or were called by, another number associated with terrorism.[97] In rare cases, the NSA can make a third "hop" to the next layer of connections.[98] Assuming that every phone number has been in contact with 100 different phone numbers in the past five years, the second hop will potentially "produce a list of 10,000 phone numbers," and the third hop might produce approximately one million phone numbers.[99]

The telecommunications providers subject to these FISC orders did not previously collect and retain this data for purely business purposes.[100] This contrasts the NSA's database with the pen register at issue in *Smith*.[101] The pen register in *Smith* collected only forward-looking data on a target that the phone company already maintained for billing purposes.[102] Under FCC regulations, applicable to all common carrier phone services since the 1980's, any carrier that offers toll telephone services must retain billing

---

93. *Id.* (internal quotation marks omitted). As of late 2013, when running a query, agents may only see whether the "seed" number has called, or been called by, a phone number associated with terrorist activities; if no such associated numbers are connected to the "seed," the database does not produce a result. Geoffrey R. Stone, Professor, Univ. of Chi. Law Sch., Address to the Chicago Lawyer Chapter of the American Constitution Society and the American Civil Liberties Union of Illinois: Liberty and Security in a Changing World (Feb. 3, 2014).

94. Stone, *supra* note 80.

95. *Id.*

96. *Id.*

97. *Id.*

98. *Id.*

99. *Id.* It is worth noting, however, that while the potential size of these searches is enormous, the program had experienced limited success as of 2012, the last year for which full data was available; of the 288 queries that year, the NSA generated only twelve "tips" that it referred to the FBI for further investigation. *Id.*

100. *Klayman*, 957 F. Supp. 2d at 14-16 (explaining the retention and collection of telecommunication companies "business records").

101. *Id.* at 32.

102. *Id.*

information about all toll calls for eighteen months.[103] In contrast, the data those carriers are required to provide under the FISC order is both longer term—covering a period of five years—and more specific—including information on call completion and possibly the user's location.[104] The NSA has essentially enlisted a third party to collect data specifically for law enforcement purposes, a sort of "joint intelligence gathering operation with the government."[105]

III. CAN THE MOSAIC THEORY OF THE FOURTH AMENDMENT DISTINGUISH DATA DRAGNETS FROM THE SIMPLE PEN REGISTER USED IN *SMITH*?

To date, two District Courts have addressed the constitutionality of the NSA's telephony metadata collection program.[106] Those courts

---

103. 47 C.F.R. § 42.6 (1986). This information includes the numbers called, date, time, and length of the calls. *Id.*

104. *Klayman*, 957 F. Supp. 2d at 35-36 n. 57.

105. *Id.* at 33 ("It's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our citizens expect all phone companies to operate what is effectively a joint intelligence gathering operation with the Government."). Although not the focus of this article, some commentators contend that such an "initiatory intrusion" into the lives of citizens generally, rather than a government intrusion initiated in response to some suspicious behavior, poses the gravest possible threat to the Fourth Amendment's core values. Sundby, *supra* note 21, at 1787.

106. *See* ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); *Klayman*, 957 F. Supp. 2d 1 (D.D.C. 2013). The Second Circuit Court of Appeals also denounced the program, albeit on statutory grounds. *See* ACLU v. Clapper, 785 F.3d 787, 824 (2d Cir. 2015) ("Because we conclude that the challenged program was not authorized by the statute on which the government bases its claim of legal authority, we need not and do not reach these weighty constitutional issues."). Because this article focuses on the constitutional limits of data dragnets, I do not discuss the Second Circuit's opinion regarding the statutory structure of Section 215 of the Patriot Act.

In a declassified opinion, FISC expressed its vociferous disagreement with Judge Richard J. Leon's opinion that distinguished *Smith* from the NSA's telephony metadata program. *See In re* Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things, No. BR 14-01, at *17 (F.I.S.C. Mar. 20, 2014), https://www.documentcloud.org/documents/1148902-br-14-01-opinion-and-order.html. The court noted that:

> Judge Leon's concerns regarding NSA's retention and analysis of the call detail records are irrelevant in determining whether a Fourth Amendment search has occurred. For the same reason, Judge Leon's assertions regarding citizens' expectations with respect to the 'relationship . . . between the government and the telecom companies' also provide no basis for departing from *Smith*.

have reached diametrically opposed conclusions, due largely to differing opinions on the applicability of *Smith*.[107] Both courts showed trepidation towards blindly following the bright-line rule of the third-party doctrine, as outlined in *Smith*, in data dragnet cases.[108] Ultimately, though, they differed in their utilization of that decision. Judge William H. Pauley III held that the case was controlled by the "clear precedent" of *Smith*, a Supreme Court precedent it was honor-bound to follow by traditional notions of *stare decisis* and the hierarchy of the federal judiciary.[109] Judge Richard J. Leon, on the other hand, contended that *Smith* failed to address the precise factual scenario presented by the NSA's program, which concerns "evolutions in the Government's surveillance capabilities" unimaginable to the *Smith* court.[110] Their respective decisions illustrate the problems inimical to adapting the Constitution, and specifically the Fourth Amendment, to modern data dragnets like the NSA's.[111]

Id. (citations omitted).

107. *Compare Clapper*, 959 F. Supp. 2d at 752 (quoting Agostini v. Felton, 521 U.S. 203, 237 (1997)) ("[T]he Supreme Court did not overrule *Smith*. And the Supreme Court has instructed lower courts not to predict whether it would overrule a precedent even if its reasoning has been supplanted by later cases . . . Clear precedent applies because *Smith* held that a subscriber has no legitimate expectation of privacy in telephony metadata created by third parties. Inferior courts are bound by that precedent.") *with Klayman*, 957 F. Supp. 2d at 31 ("[T]he question in this case can more properly be styled as follows: When do present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the government, is now.").

108. Although Judge Pauley acknowledged that the Supreme Court's decision in *United States v. Jones* questioned *Smith*, he noted that "the Supreme Court did not overrule *Smith*. And the Supreme Court has instructed lower courts not to predict whether it would overrule a precedent even if its reasoning has been supplanted by later cases." *Clapper*, 959 F. Supp. 2d at 752. And arguably, Judge Leon felt that *Smith* did not apply to the NSA's program at all. *See Klayman*, 957 F. Supp. 2d at 31.

109. *Clapper*, 959 F. Supp. 2d at 752.

110. *Klayman*, 957 F. Supp. 2d at 31. Subsequent to the issuance of these two District Court opinions, FISC itself declassified a ruling that rejected one telephone company's effort to lift the order requiring it to disclose phone records to the NSA based upon Judge Leon's ruling. *See In re* Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things, No. BR 14-01, at *1-2 (F.I.S.C. Mar. 20, 2014), https://www.documentcloud.org/documents/1148902-br-14-01-opinion-and-order.html.

111. "It is that issue—how should a lower court judge apply a Supreme Court precedent in the face of changed circumstances?—that was at the core of the

The NSA's reliance upon *Smith* to justify its program is at least straightforwardly logical. Similar to the pen register in *Smith*, the NSA's program accesses information about telephone numbers dialed without accessing the content of those calls, albeit on a much grander scale.[112] But there are strong arguments to distinguish *Smith* from such a massive data dragnet that seize upon the *Smith* court's failure to foresee evolving technologies.[113]

A. The Contours of the Mosaic Theory

One distinction that has gained popularity in the lower courts is based on the "mosaic theory" (sometimes also called the "quantitative theory") of the Fourth Amendment.[114] This theory has arguably grown roots in the recent *United States v. Jones* decision, where a majority of the Justices "clearly indicated an interest in considering how the principle recognized in *Smith* should apply in a very different technological society from the one that existed in the 1970s."[115]

In *Jones*, police officers installed a GPS device on the defendant's car.[116] The officers obtained a warrant to install the device within ten days of the warrant's issuance, and within the District of Columbia; however, officers installed the device eleven days later at a parking lot in suburban Maryland.[117] The device tracked the movements of the defendant's car for twenty-eight consecutive days,

---

disagreement between the two judges. This is *always* a vexing question." Geoffrey R. Stone, *Is the NSA's Bulk Telephony Metadata Program Constitutional?*, HUFFINGTON POST (Jan. 3, 2014, 3:17 PM), www.huffingtonpost.com/geoffrey-r-stone/is-the-nsas-bulk-telephon_b_4538173.html (alteration in original).

112. Stone, *supra* note 80.

113. "We might attribute the holding in *Smith* to the fact that it was decided almost three decades ago, at a time when members of the Court were presumably unaware of the potential for, and consequences of, mining data from transactions mediated by evolving technologies." Brenner & Clarke, *supra* note 39, at 252-53. Brenner and Clarke use this insight to critique the Court's jurisprudence regarding data collected by online companies that could be seized by the government without a warrant under *Smith*. *Id.* at 258. They argue that the transfer of digital information is not a "disclosure" to a third party in the same way that confiding in a person is a disclosure. *Id.* at 257-58. Not all disclosures are equal—some are expressly confidential, such as many online arrangements—and the Supreme Court should respect that. *Id.*

114. *See* United States v. Maynard, 615 F.3d 544, 558-65 (D.C. Cir. 2010); Mont. State Fund v. Simms, 270 P.3d 64, 69-72 (Mont. 2012) (Nelson, J., concurring).

115. Stone, *supra* note 6.

116. United States v. Jones, 132 S. Ct. 945, 948 (2012).

117. *Id.*

tying the defendant to a drug conspiracy.[118] The defendant moved to suppress the GPS evidence as gathered in violation of the Fourth Amendment, which he claimed required a valid warrant.[119]

While the Court resolved *Jones* by finding that the police searched the defendant because physically installing the GPS device constituted a trespass,[120] there was support amongst the Justices for the mosaic theory.[121] Under that approach, even though citizens have no expectation of privacy on public streets, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy," and constitute a search.[122] At some point, constant and ubiquitous monitoring infringes upon privacy in a way that individual instances of the same monitoring do not.[123] As Gray and Citron have put it, "[t]he fundamental insight behind the mosaic theory is that we can maintain reasonable expectations of Fourth Amendment privacy in certain quantities of information and data even if we lack reasonable expectations of privacy in the constituent parts of that whole."[124] Under this theory, "[i]dentifying Fourth Amendment searches requires analyzing police actions over time as a collective 'mosaic' of surveillance; the mosaic can count as a collective Fourth Amendment search even though the individual steps taken in isolation do not."[125]

The mosaic theory, if valid, would arguably control the case of the NSA's telephone dragnet; Judge Leon's recent decision provides some useful guidance.[126] Judge Leon noted that the pen register in

---

118. *Id.*

119. *Id.* at 948-49.

120. *Id.* at 951-54.

121. Justice Alito voiced support for the theory in an opinion joined by Justices Ginsberg, Breyer, and Kagan, while Justice Sotomayor sounded sympathetic tones in a concurring opinion. *Id.* at 957 (Alito, J., concurring); *Id.* at 954 (Sotomayor, J., concurring).

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

123. *See* Stone, *supra* note 6 ("The critical distinction, Justice Alito reasoned, was that, for practical reasons, the police cannot physically 'monitor and catalogue every single movement of an individual's car for a very long period.' The traditional form of surveillance—following the person—is realistic only in extraordinary circumstances. . . . The advent of GPS, however, has changed the situation dramatically, and individuals, he concluded, do have a reasonable expectation of privacy that the police will not use this new technology without restraint to track their every move.").

124. Gray & Citron, *A Shattered Looking Glass*, *supra* note 6, at 390; *see also* Gray & Citron, *Quantitative Privacy*, *supra* note 6, at 68-69.

125. Kerr, *supra* note 5, at 313.

126. *See Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013); Stone, *supra* note 6 ("Judge Leon was right that the use of the pen register in *Smith* was a far cry from

Smith was only operational for a few days, and the records were presumably discarded shortly thereafter.[127] The NSA's program involves "the creation and maintenance of a historical database containing five years' worth of data," and "will go on for as long as America is combating terrorism, which realistically could be forever!"[128] Furthermore, with the onset of cell phones, there are far more numbers to be mined than there were at the time of *Smith*.[129] Indeed:

> According to the 1979 U.S. Census, in that year, 71,958,000 homes had telephones available, while 6,614,000 did not. In December 2012, there were a whopping 326,475,248 mobile subscriber connections in the United States, of which approximately 304 million were for phones and twenty-two million were for computers, tablets, and modems.[130]

The framework for an argument that the NSA's telephony metadata collection program constitutes a mosaic search is thus relatively clear. Although each individual data point obtained is not a search under *Smith*, the quantitative whole of all the data concerning phone numbers dialed over a five-year period paints such a detailed mosaic of one's life that it invades one's reasonable expectations of privacy and constitutes a search.

The mosaic theory, however, would open the door to a host of practical problems caused by its complexity and opacity. Orin Kerr has summarized the potential pitfalls nicely:

---

the NSA's bulk telephony meta-data program in terms of the scale of its invasion of individual privacy.").

127. *Klayman*, 957 F. Supp. 2d at 32.

128. *Id.* (emphasis omitted). The NSA's program is thus historical rather than forward-looking, captures data over a period of five years rather than a few days, and could be continued forever rather than being snuffed out after a brief period. *Id.* Judge Leon also emphasized that telephone carriers have essentially been ordered to *keep* certain information rather than simply *disclose* information they already maintained. *Id.*

129. *Id.* at 33-34.

130. *Id.* at 34 (citations omitted) (noting that the global total of mobile subscribers is approximately 6.6 billion). Judge Leon also emphasized the differences between the information collected by a pen register and that obtained by the NSA. *Id.* at 34-35. While the former simply "recorded numbers on a paper tape, and did not even reveal whether the call went through, let alone how long it lasted," Freiwald, *supra* note 86, at 71, the NSA's program collects considerably more information, including whether the call was completed, the call's duration, and possibly even the user's location. *Klayman*, 957 F. Supp. 2d at 35 n.57.

> [W]hat is the standard for the mosaic? How should courts aggregate conduct to know when a sufficient mosaic has been created? What techniques should fall within the mosaic approach? Should mosaic searches require a warrant? If so, how can mosaic warrants satisfy the particularity requirement? Should the exclusionary rule apply to violations of the mosaic search doctrine? Who has standing to challenge mosaic searches?[131]

Although these hurdles to creating a mosaic doctrine in the Fourth Amendment are high, they are manageable through the normal course of jurisprudential development. Existing Fourth Amendment law is no stranger to the kind of intricate and often circumstantial tests that courts would need to develop to implement the mosaic theory.[132] Mosaic theorists can argue that the judiciary could develop answers to Kerr's challenges if the Supreme Court officially adopted their quantitative view of Fourth Amendment searches.[133]

Although the mosaic theory is attractive, one critique is particularly troubling: insofar as it accepts *Smith* as a valid

---

131. Kerr, *supra* note 5, at 314.

132. Fourth Amendment jurisprudence is replete with abstract constitutional tests. Any principle of law whose "animating core . . . is reasonableness" will require skillful judicial line-drawing. Gray & Citron, *A Shattered Looking Glass*, *supra* note 6, at 423-24 (highlighting the endemic line-drawing problems in Fourth Amendment jurisprudence, including, most prominently, questions of reasonableness and probable cause).

133. One suggestion to overcome these hurdles is Gray and Citron's approach to mosaic theory. *See* Gray & Citron, *Quantitative Privacy*, *supra* note 6, at 101-02. They focus on technology utilized by the government to determine when a search violates the Fourth Amendment. The Fourth Amendment should apply to any "investigative technique of technology [that] has the capacity to facilitate broad programs of indiscriminate surveillance that raise the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of government." *Id.* at 101. This would include the NSA's dragnet:

> By virtue of their scale and scope, these data aggregation capacities epitomize a surveillance state when put at the service of the government. Verizon's use of these technologies at the behest of government agencies should therefore be subject to Fourth Amendment regulation.

Id. at 143. This view addresses some of the practical problems facing mosaic theory, though it does not answer them all.

precedent to be distinguished on its facts,[134] mosaic theory violates arithmetic by suggesting that some quantity of non-searches equals a search.[135] The D.C. Circuit noted this issue in the *Jones*: "[t]he 'sum of an infinite number of zero-value parts is also zero.'"[136] Yet mosaic theorists suggest the opposite, arguing that even though an individual government action does not rise to the level of a search, enough non-searches equate to a search.[137] Indeed, they must argue not just that the whole is greater than the sum of its parts, but that the whole is somehow greater than nothing.

Of course, mosaic theorists could answer that the government's collection of data disclosed to third parties is a small invasion of privacy that can be aggregated to constitute a search. That, however, would require the Court to overrule third-party-doctrine cases like *Smith* and *Miller*.[138] Remember, the third-party doctrine suggests that a citizen maintains *no* reasonable expectation of privacy in her individual disclosures to a third party, such as the numbers she dials on her phone and transmits to her phone company.[139] With the third-party doctrine in place, then, she cannot maintain any expectation of privacy in the accumulation of those disclosures.

Mosaic theorists might respond that the theory is not reducible to a mathematical equation, effectively accepting that, a in the realm of Fourth Amendment jurisprudence, a collection of zeros can somehow add up to one.[140] But this admits too much. If the mosaic theory is not reducible to a logically coherent argument, it is nothing more than judicial wizardry, incomprehensible to citizens and law

---

134. As I discuss in the next paragraph and in Part V, mosaic theorists could insist that *Smith* be overruled outright, an argument that is less likely to succeed than a straightforward claim for mosaic theory.

135. To put the problem another way, if the government only seeks information "not otherwise worthy of the protection [of the Fourth Amendment], it seems no justification for requiring probable cause to say that 'we know you *could* acquire so much third-party information from existing records that we are going to require a warrant even for this minimal request.'" Henderson, *supra* note 8, at 1023 (alteration in original) (citation omitted).

136. Gray & Citron, *A Shattered Looking Glass*, *supra* note 6, at 399 (quoting United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, J., dissenting)).

137. Kerr, *supra* note 5, at 313 ("[T]he mosaic can count as a collective Fourth Amendment search even though the individual steps taken in isolation do not.").

138. Mosaic theorists can argue that *Smith* should be outright overruled; but, as I detail below, the hurdles to overruling *Smith* under the Supreme Court's most recent expression of *stare decisis* are likely insurmountable, rendering such an argument unappealing. *See infra* Part V; *see also* Kerr, *supra* note 39, at 575-76.

139. *See* Smith v. Maryland, 442 U.S. 735, 735-36 (1979).

140. For an example of this defense, see Gray & Citron, *A Shattered Looking Glass*, *supra* note 6, at 415.

enforcement agents. The Fourth Amendment loses its efficacy if it becomes too convoluted to provide guidance for the parties that apply it. "Muddy and unpredictable tests are both unfair and ultimately fail to provide substantial protection. From a more theoretical perspective, failure to provide fair warning may, as Lon Fuller has argued, constitute a failure to make law in the first place."[141]

IV. HOW TRANQUILITY CAN SAVE THE MOSAIC THEORY

The mosaic theory appears to have struck a chord with several Supreme Court Justices and provided doctrinal justification for finding that data dragnets are Fourth Amendment searches. But its mathematical flaw may prevent it from distinguishing data dragnets from the information collected in third-party-doctrine cases. However, the flaw may be resolved without relying upon mystical judicial perceptions.

The alternative I propose is a collective Fourth Amendment interest shared by citizens utilizing telecom services that are infringed upon by data dragnets.[142] The collective interest is not based upon privacy, which is inherently personal and not shared with humanity.[143] Instead, it is derived from constitutional tranquility—an ideal woven into the Constitution's structure and implicit in Justice Brandeis's expression of the Fourth Amendment as the "right to be let alone."[144] I believe that this approach is more attractive than a direct assault on third-party doctrine cases like *Smith* and *Miller*. This Part discusses my tranquility supplement to

---

141. *Id.* at 409 (citing LON FULLER, THE MORALITY OF LAW 33-39 (2d ed. 1964)).

142. The collective nature of constitutional tranquility bears some resemblance to the "social interests" of Roscoe Pound, a type of "claim[] or demand[] or desire[] involved in social life in civilized society and asserted in title of that life" which can be treated as "the claims of the whole social group as such." Roscoe Pound, *A Survey of Social Interests*, 57 HARV. L. REV. 1, 2 (1943); *see also* ROSCOE POUND, SOCIAL CONTROL THROUGH LAW (1942). Although Pound emphasized the importance of "[t]he social interest in general security," he also gave pride of place to those public policies "against things tending to oppression," a potentially apt description of government policies that violate constitutional tranquility. Pound, *A Survey of Social Interests*, *supra*, at 8.

143. The third-party doctrine assumes as much; it holds that once another person is privy to your personal information, it is no longer private. *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").

144. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

the mosaic theory, and the following Part suggests why that argument should be more appealing to mosaic theorists than directly overruling the third-party doctrine.[145]

Tranquility is one of the overarching purposes of the Constitution, given expression in its preamble, promising to "insure domestic Tranquility."[146] But constitutional tranquility is an under-theorized concept. It implies a level of peace and quiet in our daily affairs, and suggests that the default position of government is one of inaction, not aggressive intrusion into citizens' lives. A citizen has the right to lead a tranquil life, to rest assured that the government will not needlessly harass her, and this is true whether such harassment is conspicuous or covert. It makes no difference if the government effort is unknown to citizens; the tranquil foundation of life in a free republic is disrupted by the activity itself, not by its effect upon citizens' consciousness.[147] The disruption impairs constitutional tranquility.

This gives the concept of tranquility some advantages over the expectation of privacy standard that has been the touchstone of Fourth Amendment jurisprudence.[148] A citizen's expectation of privacy is based on her perception, of what she considers her slice of the world, upon which no one can intrude without her permission, or a court's prior approval. By contrast, a citizen's interest in tranquility is based on reality, rather than perception. Whether or not she believes the government should access certain information, or is capable of collecting such information, the reality that the information *is* being collected creates a disturbance of constitutional tranquility. The government activity may not violate a reasonable expectation of privacy, and thus the accumulation of these non-invasions does not amount to an invasion of privacy. But, each government action is an infringement upon the tranquility implicit in the Fourth Amendment, and a sufficient aggregation of such infringements is a search.

---

145. *See infra* Part V.

146. U.S. CONST. pmbl.

147. Tranquility is akin to an intentional tort such as battery. *See* RESTATEMENT (SECOND) OF TORTS § 18 (Am. Law Inst. 1965). Just as the victim of a battery need not be conscious of the tortfeasor's act to later bring suit, a citizen need not be aware of a government program's existence to later challenge that invasion in court. *See id.* § 18 cmt. d ("In order that the actor may be liable . . . it is not necessary that the other should know of the offensive contact which is inflicted upon him at the time when it is inflicted.").

148. *See* California v. Ciraolo, 476 U.S. 207, 211 (1986) (explaining that the "reasonable expectation of privacy" test is the "touchstone of Fourth Amendment analysis").

Though constitutional tranquility is an under-theorized concept, its basic contours are echoed in Justice Brandeis's understanding of the Fourth Amendment.[149] Brandeis also situated the amendment's protections in the broader context of the American Constitutional project; borrowing from the Declaration of Independence, Brandeis asserted that "[t]he makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness."[150] The makers' aim could only be achieved if they established the right to be let alone—"the most comprehensive of rights, and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[151] Arguably, Brandeis's declaration was an exhortation for the Court not to forsake tranquility in Fourth Amendment jurisprudence. It was a reminder not to allow government actors to disturb the peace and quiet of citizens' domestic lives at will.

Constitutional tranquility is reflected in the text beyond the Fourth Amendment.[152] As the Court noted in *Katz*, "The Third Amendment's prohibition against the unconsented peacetime quartering of soldiers protects another aspect of privacy from governmental intrusion."[153] Even more, "[t]o some extent, the Fifth Amendment too 'reflects the Constitution's concern for the right of each individual to a private enclave where he may lead a private life.'"[154] These textual assurances depend on a baseline level of undisturbed domestic tranquility.

Constitutional tranquility, as I have outlined it, explains our intuitive discomfort with data dragnets better than *Katz*-ian notions of privacy. It is simply untrue that we expect information we disclose to third parties will be kept private, even when that data is aggregated and packaged for delivery to another entity.[155] As

---

149. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (equating the Fourth Amendment with the "right to be let alone").

150. *Id.*

151. *Id.* at 478-79.

152. *See, e.g.*, U.S. CONST. amend. III ("No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."). Protecting the privacy of the home indicates the framer's intent to further guard against unwarranted governmental intrusion. *Id.*

153. Katz v. United States, 389 U.S. 347, 350 n.5 (1967).

154. *Id.* (quoting Tehan v. United States *ex rel.* Shott, 382 U.S. 406, 416 (1966)).

155. As Brenner and Clarke have noted, and I highlighted earlier, citizens expect that information about them is available for corporate consumption in the modern world. *See* Brenner & Clarke, *supra* note 39, at 219.

citizens well know, private advertising agencies, or companies' internal marketing departments, mine the trove of data made available through communication technology, to the point that most information about ourselves is public.[156] But government agents must restrain themselves from invading the tranquility of our daily lives until the government obtains a warrant or probable cause.[157]

Constitutional tranquility can also resolve the mathematical flaw in the mosaic theory. Minor government harassment may fail to reach the level of a Fourth Amendment search, but it is still a greater-than-zero intrusion upon constitutional tranquility—a tranquility that is shared by the citizens of the nation as a whole. Minor disturbances of tranquility can be accumulated, to the point where government action *does* constitute a search. Each government action in a data dragnet is therefore a positive violation of constitutional tranquility, and the sum of these positive integers may sufficiently trigger Fourth Amendment protection.

For example, consider government investigators' rummaging through the trash of Citizen Doe daily. Each time the government rifles through the refuse, it is not a Fourth Amendment search because it has not invaded any reasonable expectation of privacy.[158] But each dumpster dive is unsettling to Citizen Doe's peaceful domestic environment. Each action transgresses upon her and her neighbors' enjoyment of the tranquil domestic setting that is constitutive of life in a free society. This applies whether or not Citizen Doe realizes that the government is scouring her trash, because it undermines the context necessary for a peaceful existence.

That is not to say, however, that each trash inspection constitutes a search. It may be true that if the government reviewed the contents of Doe's trash on a daily basis, the intrusion upon constitutional tranquility would still not reach the level of a Fourth Amendment search.[159] But suppose, instead, that government

---

156. For an example of the capabilities of corporate data collectors, see *Stalkers Inc.*, ECONOMIST (Sept. 13, 2014), http://www.economist.com/news/leaders/21616953-surveillance-advertising-industrys-new-business-model-privacy-needs-better.

157. *See* U.S. CONST. amend IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and *no Warrants shall issue but upon probable cause*, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.") (emphasis added).

158. Based on the Court's holding in *California v. Greenwood*, we know that a citizen has no reasonable expectation of privacy in their garage once left outside for collection. *See* California v. Greenwood, 486 U.S. 35, 43-44 (1988).

159. For present purposes, I reserve judgment on whether such a program would constitute a search under the mosaic theory augmented by tranquility. Programs

officers collected and preserved every article of trash discarded by every citizen who availed herself of public trash disposal services. Those actions, in the aggregate, have a deleterious effect on the peaceful, calm nature of our daily lives and undermine constitutional tranquility. The sum of those minor intrusions create a singular disturbance upon the joint Fourth Amendment interests of all citizens utilizing trash services and constitute a search.

As absurd as the government trash-scouring example sounds, it parallels the massive data aggregation power that the NSA unleashed through its telephony metadata program.[160] The *Smith* decision holds that no individual collection of telephone metadata invades a reasonable expectation of privacy.[161] The sum of those non-invasions cannot equal one large invasion that implicates the Fourth Amendment, but each individual collection of metadata is a transgression upon the constitutional tranquility implicit in the Fourth Amendment's right to be let alone. A collection of such small government harassments can constitute a search.

The same would hold true for government efforts to mine data and establish data dragnets. Those efforts are based on the understanding that individual citizens hold no reasonable expectation of privacy in the information the government collects, like their position on a public roadway or the contents of their trashcans.[162] But the government should tread wearily when its program captures the data of practically every citizen. Each datum collected might disrupt constitutional tranquility interests, and those disruptions can be amalgamated under the revived mosaic theory to constitute a Fourth Amendment search.

As with any Fourth Amendment standard, ease of application is a paramount concern. Citizens and law enforcement officers must receive meaningful guidance for the law to play its role in balancing liberty and security. To implement my proposal, the Supreme Court would need to delineate, with clarity, when a government activity infringes upon the collective constitutional tranquility of citizens and constitutes a search. Thus, I suggest that the Court adopt this standard: When a government information collection program

---

such as the NSA's present a worst-case example of disturbances of domestic tranquility and are an appropriate test for my theory, before its application to less-intrusive forms of government monitoring.

160. Greenwald, *supra* note 4 (describing the extent of the NSA's data collection program).

161. Smith v. Maryland, 442 U.S. 735, 745 (1979). Again, as I argue below, this decision should be distinguished rather than discarded. *See infra* Part V.

162. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 43-44 (1988) (holding that a citizen has no reasonable expectation of privacy in their trash).

captures data about practically everyone engaged in a ubiquitous activity, it infringes upon constitutional tranquility and constitutes a search. Any citizen whose tranquility was disturbed would thus have standing to challenge the government's action under the Fourth Amendment.

While the government may collect data about some citizens without implicating the Fourth Amendment, it conducts a Fourth Amendment search when it collects data about virtually all of them. This kind of government search is most likely to occur in the context of cellular telephone use, or other internet-based communication. Because nearly all citizens partake in those activities, monitoring those participants is a particularly egregious form of untoward government harassment.[163]

What would be the fate of the NSA's metadata collection program if it was treated as a Fourth Amendment search? The government could not articulate probable cause, or even a reasonable and articulable suspicion, that metadata on millions of phone users is relevant to a specific investigation.[164] The particularity requirement is simply irreconcilable with that kind of indiscriminate collection.

However, it is possible that the program meets the reasonableness requirement of the Fourth Amendment.[165] Professor Geoffrey Stone, a member of President Obama's Review Group on Intelligence and Communications Technology, suggested enlisting a private entity to collect and house the metadata, limiting its scope to a two-year span, and restricting government agents access to the data unless they obtain judicial approval based on reasonable, articulable grounds that the phone number is connected with international terrorism.[166] President Obama embraced reforms mirroring those recommendations, calling upon Congress to pass legislation revamping the program to ensure that the data was housed outside of the NSA, and that it could only be queried with court approval.[167] After extended Congressional wrangling, similar

---

163. *See generally* Klayman v. Obama, 957 F. Supp. 2d 1, 34 (D.D.C. 2013) (explaining the abundance of cellphone use today, noting that the total number of subscribers is roughly 6.6 billion).

164. *See id.* at 16 (articulating the standard for obtaining a court order for this information).

165. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (articulating the "reasonableness" prong of the Fourth Amendment test).

166. Geoffrey R. Stone, *The NSA's Telephone Metadata Program is Unconstitutional*, HUFFINGTON POST (Jan. 9, 2014, 6:59 PM), www.huffingtonpost.com/geoffrey-r-stone/the-nsas-meta-d_b_4571523.html.

167. Tom Cohen, Lisa Desjardins & Jim Acosta, *Obama, Congress working on*

reforms were enacted.[168] Combined, these reforms may alleviate the constitutional concerns raised by the program's intrusion upon Fourth Amendment rights because the government is no longer in the business of directly collecting data, indiscriminately, on millions of Americans.[169] Instead, the government can only access a third party's telephony data upon a showing of reasonable, articulable suspicion about a particular phone number, which may be all the Fourth Amendment requires.[170]

V. SHOULD *SMITH* BE DIRECTLY OVERRULED?

It is worth considering whether advocates should bother with an argument that factually distinguishes data dragnets from the government activities at issue in *Smith*, and in other third-party doctrine cases.[171] In this Part, I counsel against such an alternative. First, the Court's current *stare decisis* doctrine does not provide a convincing justification to overrule *Smith*.[172] Second, the rules *Smith*

---

changes to NSA, CNN (Mar. 25, 2014), http://www.cnn.com/2014/03/25/politics/white-house-nsa/. House Intelligence Committee chairman Mike Rogers, and ranking Democrat Dutch Ruppersberger, proposed parallel reforms to the NSA's program. Alex Rogers, *Lawmakers Float Their Own NSA Reform Bill*, TIME (Mar. 25, 2014), http://time.com/37336/lawmakers-float-their-own-nsa-reform-bill/.

168. *See* Steinbauer & Weisman, *supra* note 74. This legislation's path to passage, however, was anything but straightforward. Although legislation passed by the House, known as the USA Freedom Act, contained a diluted form of the President's proposals, including the need for a query to be tied to a specific phone number associated with terrorism, the proposal failed to gain enough support in the Senate. Charlie Savage & Jeremy W. Peters, *Bill to Restrict N.S.A. Data Collection Blocked in Vote by Senate Republicans*, N.Y. TIMES (Nov. 18, 2014), http://www.nytimes.com/2014/11/19/us/nsa-phone-records.html?_r=0; *see also House Curbs NSA Data Collection*, POLITICO (May 22, 2014), http://www.politico.com/story/2014/05/congress-nsa-data-collection-106994. Jonathan Weisman & Charlie Savage, *House Passes Restraints on Bulk Data Collection*, N.Y. TIMES (May 22, 2014), http://www.nytimes.com/2014/05/23/us/politics/house-votes-to-limit-nsas-collection-of-phone-data.html?hp. It was not until the summer of 2015, and after extended hand-wringing by Senate Majority Leader Mitch McConnell and civil liberties gadfly Rand Paul, that these reforms passed into law. *See* Steinbauer & Weisman, *supra* note 74.

169. *See* Steinbauer & Weisman, *supra* note 74 (explaining the new restrictions on data collection).

170. Whether the warrant requirement would be triggered by the NSA's program is a worthwhile question, but is beyond the scope of the current paper.

171. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 741 (1979) (detailing the type and manner of information collected in the case).

172. *See infra* Part V.A.

established retain some salience on the limited facts to which they apply.[173]

A. Is Smith *Ripe for Overruling Under the Stare Decisis Doctrine?*

The Supreme Court is not likely to reverse course and strike down *Smith* and its progeny based on its current understanding of *stare decisis*.[174] In *Planned Parenthood of Southeastern Pennsylvania v. Casey*, the Court outlined four factors to consider when determining whether to apply or discard precedent:

> [(1)] whether the rule has proven to be intolerable simply in defying practical workability; [(2)] whether the rule is subject to a kind of reliance that would lend a special hardship to the consequences of overruling and add inequity to the cost of repudiation; [(3)] whether related principles of law have so far developed as to have left the old rule no more than a remnant of abandoned doctrine; or [(4), which is perhaps most importantly for the present discussion,] whether facts have so changed, or come to be seen so differently, as to have robbed the old rule of significant application or justification.[175]

Like it or not, *Smith*'s rule—that citizens have no reasonable expectation of privacy in the numbers they dial—is workable in resolving what would otherwise be a controversial field of Fourth Amendment law.[176] It draws a line that is perhaps unjustifiable, but

---

173. *See infra* Part V.B.

174. *See* Planned Parenthood of Se. Pennsylvania v. Casey, 505 U.S. 833, 854-55 (1992) (explaining the Court's stance on *stare decisis* and its importance in American jurisprudence).

175. *Id.* at 854-55 (citations omitted). These factors balanced the "contrary necessities" that define the obligation to follow precedent. *Id.* at 854. As the Court explained:

> [N]o judicial system could do society's work if it eyed each issue afresh in every case that raised it. Indeed, the very concept of the rule of law underlying our own Constitution requires such continuity over time that a respect for precedent is, by definition, indispensable. At the other extreme, a different necessity would make itself felt if a prior judicial ruling should come to be seen so clearly as error that its enforcement was for that very reason doomed.

Id. (citing BENJAMIN N. CARDOZO, THE NATURE OF THE JUDICIAL PROCESS 149 (1921)).

176. *See* Smith v. Maryland, 442 U.S. 735, 742-46 (1979).

the line is bright and easily applied.[177] Citizens have no reasonable expectation of privacy in information they disclose to a third party, and thus the government's acquisition of that information does not constitute a search under the Fourth Amendment. [178]

Next, *Smith* has generated significant reliance interests. As Kerr noted, the third-party doctrine promises government investigators access to a public-facing portion of most crimes without offending the Fourth Amendment's strictures.[179] Of course, opponents of programs such as the NSA's can contend that *Smith* does not apply to current government efforts because the information differs from that acquired by pen registers.[180] But opponents must also concede that even if *Smith* is distinguishable, it has been the law of the land, and a touchstone of law enforcement guidance, for almost forty years.[181]

Regarding the third factor of the Court's *stare decisis* doctrine, principles of law have not developed around the third-party doctrine expressed in *Smith*. In fact, *Smith*'s third-party doctrine stifled further conceptual developments in search and seizure jurisprudence.[182] Without it, a more nuanced approach to government information-gathering techniques may have emerged, one that considers individualized factors when determining reasonable expectations of privacy, and perhaps classifies government programs by the purposes for which they were created. The law has instead stagnated, with drastic consequences for emerging technologies.[183] While opponents of the third-party

---

177. *See id.*

178. *Id.* According to the Court in *Miller*, a citizen "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." United States v. Miller, 425 U.S. 435, 443 (1976). This simplistic, bright-line rule has strongly riled commentators.

179. Kerr, *supra* note 39, at 575-76. "Without the third-party doctrine, savvy wrongdoers could use third-party services in a tactical way to enshroud the entirety of their crimes in zones of Fourth Amendment protection." *Id.* at 564.

180. *Smith*, 442 U.S. at 741 (describing the type of data collected by pen registers). As noted above, current data collection includes information about call completion, call duration, and possibly indefinite preservation of the data once collected. Klayman v. Obama, 957 F. Supp. 2d 1, 35 (D.D.C. 2013).

181. As I will discuss in more detail below, there is a countervailing instinct in cases of national security and emerging technology to afford less weight to an aged precedent. *See infra* Part V.B. The special circumstances inimical to those cases counsel against preserving precedents like *Smith*. *Id.*

182. *See generally Klayman*, 957 F. Supp. 2d at 35 (noting that *Smith* "'squarely control[s]' when it comes to '[t]he production of telephone service provider metadata'") (citations omitted).

183. *See* United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kans. 2000); United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999); Freiwald, *supra*

doctrine argue that it precludes the jurisprudential flexibility needed to address privacy concerns in the face of emerging technologies, under the Court's *stare decisis* doctrine, that preclusion favors *Smith*'s preservation.[184]

The final factor—"whether facts have so changed, or come to be seen so differently, as to have robbed the old rule of significant application or justification"—offers the greatest opportunity for overruling *Smith*.[185] The law enforcement world in *Smith*—involving pen registers, or the types of listening devices considered in *Katz*—has changed dramatically.[186] Yet, at an individual level, it is arguable that the glut of data available reduced the expectation of privacy citizens hold in information provided to the entities

---

note 86, at 53 (citing Guest v. Leis, 255 F.3d 325, 335-36 (6th Cir. 2001)) ("[C]ourts have denied constitutional protection to online communication attributes, such as the user's email address and other identifying information, including passwords, [by reasoning] that users forfeit any privacy interest in such information when they voluntarily give the information to their electronic service providers."). Without *Smith*, more nuanced analysis might have also arisen regarding online retailers, who typically collect and store information to conduct market research and design targeted marketing campaigns. *See* Brenner & Clarke, *supra* note 39, at 215-16. Susan W. Brenner and Leo F. Clark suggest that citizens retain privacy interests in certain types of stored transactional data with specific characteristics. *Id.* Brenner and Clark argue that:

> [T]he Consumer is entitled to Fourth Amendment protection for Data maintained by a Collector pursuant to a confidentiality agreement and with whom the Collector has a "trust-based" relationship (with "trust-based" defined broadly and not legally), as long as the Data is maintained at least in part for the Consumer's benefit and is directly accessible by the Consumer.

Id.

184. There are reasons to avoid overruling a precedent because related principles of law have developed around the decision such that the old rule is a "remnant of abandoned doctrine." Planned Parenthood of Se. Pennsylvania v. Casey, 505 U.S. 833, 854-55 (1992). This factor can allow Justices to slowly undermine a precedent, then later claim that the original precedent should be abandoned. *See* Barry Friedman, *The Wages of Stealth Overruling (With Particular Attention to* Miranda v. Arizona*)*, 99 GEO. L.J. 1, 26, 29-30 (2010). From a Rule of Law perspective, this is a pernicious process that should be avoided. *See* Michael Gentithes, *Precedent, Humility, and Justice*, 18 TEX. WESLEYAN L. REV. 835, 884-89 (2012).

185. *Casey*, 505 U.S. at 855.

186. *See* Smith v. Maryland, 442 U.S. 735, 741 (1979) (describing the pen register); Katz v. United States, 389 U.S. 347, 348 (1967) (explaining the eavesdropping device utilized in the case).

responsible for connecting us to the modern world.[187] There is an expectation—perhaps paranoia—that nothing in our lives is private, given advances in modern technology and the desire of governments and corporations to amass this information.[188] Regarding our reasonable privacy expectations, then, *Smith* retains salience. Because each of the other *stare decisis* factors favor upholding *Smith*, and the fourth factor is a weak argument for overruling, *Smith* likely cannot be invalidated in cases concerning data dragnets.

By arguing that *Smith* is protected by *stare decisis*, I am not implying that its rationale is convincing. I strongly disagree with the Court's claim that "[d]isclosure to third parties eliminates protection [under the Fourth Amendment] because it implies consent."[189] The consent rationale fails if the disclosure of information to a third party is mandatory to function in society.[190] Consent implies a

---

187. *See* Sundby, *supra* note 21, at 1760-61. According to Sundby:

> [B]ecause the Court is not asking whether bank or phone records should be kept private (thus invoking privacy as a value), but, rather, whether we as a factual matter expect others to see and use those records (thus viewing privacy as a measurable fact), Fourth Amendment protections will shrink as our everyday expectations of privacy also diminish.

Id.

188. *See* Brenner & Clarke, *supra* note 39, at 219 ("More than ever before, the details about our lives are no longer our own. They belong to the companies that collect them, and the government agencies that buy or demand them in the name of keeping us safe."); *see also Stalkers Inc.*, *supra* note 156.

189. Kerr, *supra* note 39, at 565 ("When understood as a subset of consent law rather than an application of the reasonable expectation of privacy test, the third-party doctrine fits naturally within the rest of Fourth Amendment law."). Kerr added that "[t]hird-party disclosure eliminates privacy because the target voluntarily consents to the disclosure, not because the target's use of a third party waives a reasonable expectation of privacy." *Id.* at 587-88.

190. As Professors Brenner and Clarke put it, "[*Smith*] applies an assumption of the risk rationale to a situation in which [a citizen] actually has no choice but to forego privacy expectations unless he is willing to forego a material, if not practically essential, service." Brenner & Clarke, *supra* note 39, at 244. Brenner and Clarke note that "as computer technology becomes more embedded in society, consumers will be increasingly forced to waive their Fourth Amendment rights in order to obtain vital goods and services. We must consider, therefore, whether the Supreme Court's approach is justified." *Id.* at 245-46.

No one can consent to an activity that is necessary to preserving one's self, such as seeking medical treatment. Solove, *supra* note 30, at 1532 ("Would the Supreme Court really hold that people lack an expectation of privacy in their medical data because they convey that information to their physicians? This result would

voluntary undertaking;[191] its moral force is derived from the autonomous nature of the consentor's actions.[192] Consent must be a choice, not a condition precedent to taking a necessary action.

But as interesting as the consent critique might be, it does not rob *Smith* of applicability in data dragnet cases. Such rejoinders to *Smith* have long been presented, even in *Smith* itself.[193] The argument is essentially sour grapes over a jurisprudential battle lost long ago. Discarding precedent because it is out of academic favor goes too far; it wholly discards the guiding value those decisions have for future jurists. Judges should bring a modicum of humility to their jobs, especially when addressing longstanding precedents that resolved pressing challenges in our society, such as the balance between liberty and security in a free state.[194] This is paramount in

---

strike many as absurd."). Phone users undertake an activity necessary to acquire innumerable benefits (and avoid an untold number of burdens) in modern life. "If a disclosure is necessary to participate in society, this weighs in favor of restricting government access. In what could be considered the most extreme case, no disclosure is intended and the disclosure cannot reasonably be prevented." Henderson, *supra* note 8, at 989.

191. John Kleinig, *The Nature of Consent*, *in* THE ETHICS OF CONSENT: THEORY AND PRACTICE 14-16 (Franklin G. Miller & Alan Wertheimer eds., 2009).

192. *See* Tom L. Beauchamp, *Autonomy and Consent*, *in* THE ETHICS OF CONSENT: THEORY AND PRACTICE 55-56, 62-63, 74 (Franklin G. Miller & Alan Wertheimer eds., 2009). For a recent application of these principles to internet liability waivers and service agreements, see MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2014).

193. In dissent, Justice Marshall claimed that "unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting) (citations omitted). Even in *Miller*, Justice Brennan claimed that "[f]or all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account." United States v. Miller, 425 U.S. 435, 451 (1976) (quoting Burrows v. Superior Court, 529 P.2d 590, 596 (1974)). Brenner and Clarke also made this argument regarding online consumer relationships. Brenner & Clarke, *supra* note 39, at 262 ("The lack of meaningful choice also distinguishes the Consumer-Collector relationship from the snitch scenario that produced the holding in *Hoffa*.").

194. Gentithes, *supra* note 184, at 859, 861-62, 869. Such a humble approach to judge's work, especially on high courts, accounts for the power of precedent to perpetuate a broader cross-generational legal project and provide a useful framework for troubling legal issues amongst judicial contemporaries. *Id.* Such humility equates to a "just" decision. *Id.* at 853-860. For further discussion of the cross-generational and horizontal values of precedent, see *id.* at 860-873.

Constitutional cases, where the sparse words of the document may provide less guidance, and a far less useful framework for discussion, than the line of decisions judicial predecessors generated.[195] The Fourth Amendment is no exception. Thus, long-harbored discomfort with *Smith* is not a sufficient basis for overruling the decision.

B. Does Smith's *Age Undermine Its Validity?*

Opponents may also be tempted to discard *Smith* as jurisprudential jetsam because of its age.[196] Courts may desire to limit judge's dead-hand control over new technological advances that were unimaginable when the decision was rendered.

When data dragnets are utilized as weapons in the war on terror, several factors discussed below imply that *Smith* may be less valuable. Data dragnets fall on the intersection of national security interests and rapidly advancing technological capabilities. Where wholesale changes of circumstance are the norm, and a perpetually shifting factual background the expectation, judicial efforts to author rules of broad applicability fare poorly. This implies a reversal of the typical argument waged against precedent, where a short-lived decision might be derided as ill-conceived and quickly reversed, while a longer-standing precedent is more valued in settling legal controversies and establishing societal expectations about the laws.[197] On the contrary, an aged precedent in an area of law where national security and emerging technology intersect is likely not in lockstep with the innumerable variables that arise. Thus, a precedent's age may count against it in such cases.

Another unique factor of the NSA's program—the emergency nature of the legislation—suggests that older precedent like *Smith* should not apply. Because the precedent did not contemplate the "emergency" circumstances behind legislation like the Patriot Act, it cannot support the legislation's continuing validity.[198] "[T]he fear

---

195. *Id.* at 874-75 ("The Constitution's very indeterminacy requires reliance upon precedent to avoid the problem of Justices simply talking past one another as they engage in their interpretive project.").

196. *See* Fakhoury, *supra* note 2 (discussing the age of the case).

197. The age of a ruling may give it additional weight, but that does not render it immovable; "perhaps of equal importance is the sum of precedent behind that decision, building upon previous decisions over generations." Gentithes, *supra* note 184, at 889. "When a precedent has been repeatedly reexamined and reaffirmed, over many years by a Court whose composition has changed, that should give us greater confidence that the precedent is correct." DAVID STRAUSS, THE LIVING CONSTITUTION 96 (2010).

198. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 12 (D.D.C. 2013) (noting that the

that privacy must be reduced or there will be blood on our hands when another terrorist attack occurs generates high emotion rather than reasoned deliberation. Short-lived emotional reactions should not guide legislation designed to last."[199]

However, while *Smith*'s age might give the Supreme Court pause in applying it to data dragnet cases, the Court will likely not overrule *Smith*. Age alone is not a factor in the *stare decisis* doctrine, and traditionally a precedent's gray whiskers support its preservation. But *Smith*'s age should give the Court some pause, and perhaps provide the opening for a distinction based on the mosaic theory supplemented by constitutional tranquility. But age alone will not lead to the outright reversal of *Smith*.

CONCLUSION

In the abstract, government use of data dragnets offends basic principles of a free, liberal society. Yet the government has justified its use of data dragnets by relying on long-standing, clearly reasoned Supreme Court precedent.[200] The government's position is in error, especially considering the detailed picture its data can paint of citizens' lives. But the mosaic theory of the Fourth Amendment, as presently constructed, contains a mathematical flaw that must be overcome. This article seeks to augment the mosaic theory and correct the flaw with a proper understanding of citizens' shared interest in constitutional tranquility. The interest in constitutional tranquility explains our discomfort with government data dragnets, and why such dragnets offend Fourth Amendment principles. It thus provides a basis to argue that data dragnets constitute a search, and it can guide courts and litigants to resolve the legal ramifications of technological advances, both in the case of the NSA's telephony metadata program and beyond.

September 11th attacks necessitated the passage of the Patriot Act).

199. Freiwald, *supra* note 86, at 78 (citations omitted). "It seems clear that the terrorist threat will plague us for the foreseeable future. Realigning our rights to contend with terrorism must work in the long-term rather than be a short-term fix." *Id.* To date, there is no proof that the NSA's program has stopped any terrorist attacks. *See* Klayman, 957 F. Supp. 2d at 40. "Before we are convinced otherwise, we should see specific cases in which fishing through the data of those not suspected of terrorist activity yields useful data that is worth the cost in resources and privacy." Freiwald, *supra* note 86, at 83 (citations omitted). "The experts tell us that such fishing expeditions will be fruitless. History tells us that providing the government with broad surveillance powers could have a drastic impact on our freedoms and democracy." *Id.*

200. *See* Smith v. Maryland, 442 U.S. 735, 742-46 (1979).