UIC John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 2 Article 3

2014

Bulk Telephony Metadata Collection and the Fourth Amendment: The Case For Revisiting the Third-Party Disclosure Doctrine in the Digital Age, 31 J. Marshall J. Info. Tech. & Privacy L. 191 (2014)

Timothy Geverd

BULK TELEPHONY METADATA COLLECTION AND THE FOURTH AMENDMENT: THE CASE FOR REVISITING THE THIRD-PARTY DISCLOSURE DOCTRINE IN THE DIGITAL AGE

TIMOTHY J. GEVERD*

"[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."[1]

INTRODUCTION

On June 5, 2013, Glenn Greenwald of *The Guardian* reported on leaked National Security Agency ("NSA") documents revealing that the Agency was "collecting the telephone records of millions of US customers. . . under a top secret order issued in April."[2] On June 9, 2013, *The Guardian* released the identity of the source of the NSA leaks as Edward Snowden.[3] Snowden, claiming that the NSA surveillance programs "pose[] 'an existential threat to democracy,'"[4] leaked the top secret documents in order "' . . . to inform the public as to that which is

* Law Clerk, The Honorable B. Avant Edenfield, United States District Court for the Southern District of Georgia (2014-15 Term). Special thanks to Dean Craig Lerner of George Mason University School of Law for his invaluable insight throughout the writing of this Article and to my good friend Joseph Oliveri for his thoughtful edits and comments. All views expressed here are my own, as are any errors.

1. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

2. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 5, 2013) [hereinafter Greenwald, *Verizon*], http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

3. Glenn Greenwald, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 9, 2013), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

4. *Id.*

done in their name and that which is done against them'"—i.e., government use of dragnet surveillance to destroy "basic liberties."[5] Snowden recently appeared by videoconference at the South by Southwest Conference in Austin, Texas.[6] When asked if he would leak the details of the NSA surveillance programs again if given the chance, Snowden responded, "'Absolutely yes," and added "that he 'took an oath to support and defend the Constitution and [he] saw the Constitution . . . being violated on a massive scale.'"[7] However, it is far from clear that the NSA's surveillance programs do indeed violate the Constitution under current Fourth Amendment principles.

Despite the Fourth Amendment's guarantee that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated,"[8] the United States Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information voluntarily turned over to third parties."[9] Thus, information disclosed to third parties falls outside of the protection of the Fourth Amendment. Under this third-party disclosure doctrine, the Court has held that the phone numbers one dials are beyond the scope of Fourth Amendment protection.[10] Similarly, lower federal courts have applied the third-party disclosure doctrine to power records produced by utility companies,[11] to records kept by Inter-

---

5. *Id.*

6. *E.g.*, Brandon Griggs & Doug Gross, *Edward Snowden Speaks at SXSW, Calls for Public Oversight of U.S. Spy Programs*, CNN (Mar. 10, 2014, 8:39 PM), http://www.cnn.com/2014/03/10/tech/web/edward-snowden-sxsw (noting that "[t]he event marked the first time the former National Security Agency contractor . . . directly addressed people in the United States since he fled the country with thousands of secret documents").

7. Mark Memmott, *Edward Snowden Tells SXSW He'd Leak Those Secrets Again*, NPR (Mar. 10, 2014, 12:11 PM), http://www.npr.org/blogs/thetwo-way/2014/03/10/288601356/live-edward-snowden-speaks-to-sxsw.

8. U.S. CONST. amend. IV.

9. *E.g.*, Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (citing cases). Lower federal courts continue to cite *Smith* approvingly. *See*, *e.g.*, United States v. Flores-Lopez, 670 F.3d 803, 807 (7th Cir. 2012) ("[O]btaining [a phone number] from the phone company isn't a search because by subscribing to the telephone service the user of the phone is deemed to surrender any privacy interest he may have had in his number.").

10. *Smith*, 442 U.S. at 745-46.

11. *E.g.*, United States v. McIntyre, 646 F.3d 1107, 1111-12 (8th Cir. 2011); *see also* United States v. Porco, 842 F. Supp. 1393, 1398 (D. Wyo. 1994) ("[T]he defendants had no legitimate expectation of privacy in Rural Electric records of the electrical usage at their residence," because they "chose to use electricity provided by Rural Electric and knew that their electrical usage was monitored by Rural Electric in order to generate a monthly bill").

net Service Providers ("ISPs"), [12] and to credit card information.[13]

The third-party disclosure doctrine thus clears the way for broad surveillance programs like the ones Edward Snowden leaked, capturing the attention of the American people and the world. Lack of constitutional protection for such information certainly is cause for alarm in today's digital world. Simply put, "your privacy is not Fourth Amendment safe" in the digital age.[14] For many years, electronic surveillance has been beyond the reach of federal courts, because "[o]nce [information is] disclosed, that is the end of the privacy inquiry, and the result is that privacy protection is lost" regardless of "the circumstances surrounding that disclosure."[15] However, in the wake of the Edward Snowden leaks, federal courts will be forced to consider the continued vitality of the third-party disclosure doctrine in today's technological age. [16]

Thus far, three United States District Courts have considered the legality of the NSA's bulk data collection and have reached conflicting

---

12. *E.g.*, United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (concluding that "computer surveillance techniques that reveal the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account" is "constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*"); *see also, e.g.*, United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address [Fourth Amendment protection of Internet subscriber information] has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation." (citing cases)).

13. *See, e.g.*, United States v. Alabi, 943 F. Supp. 2d 1201, 1207 (D.N.M. 2013) ("The government's scan of credit card and debit cards' magnetic strips is . . . not a Fourth Amendment search under the reasonable-expectation-of-privacy approach . . . , because . . . given that the electronically stored account information is necessarily disclosed to private parties when credit and debit cards are used as intended, the scan does not implicate a legitimate privacy interest.").

14. *See* Grover G. Norquist & Laura Murphy, Opinion, *A Fourth Amendment Application for the Internet*, POLITICO (Mar. 17, 2013, 9:40 PM), http://www.politico.com/story/2013/03/grover-norquist-laura-murphy-a-fourth-amendment-application-for-the-internet-88955.html.

15. Samuel Mark Borowski, Aaron Midler & Pervin Taleyarkhan, *Evolving Technology & Privacy Law: Can the Fourth Amendment Catch Up?*, ABA SCITECH LAW., Spring 2012, at 14, 16.

16. *See* Brendan Sasso, *Snowden Leaks Help NSA Critics in Government Surveillance Lawsuits*, THEHILL (Sept. 21, 2013, 9:27 PM), http://thehill.com/blogs/hillicon-valley/technology/323793-snowden-leaks-help-nsa-critics-in-legal-fights (noting that the Snowden leaks "eroded the government's key legal defense and could mean that questions over whether the National Security Agency is breaking the law will be decided in open court"); *see also* Klayman v. Obama, 957 F. Supp. 2d 1, 11 (D.D.C. 2013) ("Soon after the [Snowden leaks] in the news media, plaintiffs filed their complaints . . . alleging that the Government, with participation of private companies, is conducting 'a secret and illegal government scheme to intercept and analyze vast quantities of domestic telephonic communications," and "of communications from the Internet and electronic service providers." (internal citations omitted)).

conclusions.[17] Three United States Courts of Appeals have since heard oral argument on the constitutionality of the bulk telephony collection program.[18] This Article argues that federal courts should seize the opportunity presented by the Snowden leaks to reexamine the continued vitality of the current third-party disclosure doctrine in Fourth Amendment jurisprudence. Specifically, this Article argues that *Smith v. Maryland*[19] simply cannot continue to act as the "North Star" for judges navigating the "Fourth Amendment waters" of the digital age,[20] and that instead, *Smith* should apply more narrowly in the digital age. In so arguing, this Article advocates that courts apply a modified, two-step test to evaluating third-party disclosures rather than applying the traditional binary rubric that courts have drawn from *Smith* and *United States v. Miller*[21]—i.e., if information is disclosed, that information is unprotected. Thus, this Article suggests that courts ask, first, what individuals reasonably expect the scope of their disclosure to be and, second, whether a particular surveillance program is capable of revealing information beyond what those individuals reasonably expected to reveal. If the technology reveals information beyond that which individuals reasonably expected to reveal, then the use of such technology implicates the Fourth Amendment.

Part I of this Article introduces and discusses the Court's third-party disclosure doctrine as it applies to Fourth Amendment analysis. Part II then discusses Congressional regulation of electronic surveillance and introduces the NSA bulk telephony metadata collection program conducted under authority of Section 215 of the USA Patriot Act. Part III continues by discussing the three district court decisions to consider the constitutionality of the bulk telephony metadata collection program. Part IV then introduces the Supreme Court of the United

---

17. Smith v. Obama, No. 2:13-CV-257, 2014 WL 2506421, at *4 (D. Idaho June, 3 2014) ("*Smith* was not overruled, and it continues . . . to bind this Court."); ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013) ("Because *Smith* controls, the NSA's bulk telephony metadata collection program does not violate the Fourth Amendment."); *Klayman*, 957 F. Supp. 2d at 37 (distinguishing *Smith* in light of changes in technology and concluding that "it is significantly likely" that "people have a reasonable expectation of privacy that is violated when the Government, without any basis whatsoever to suspect them of any wrongdoing, collects and stores for five years their telephony metadata for purposes of subjecting it to high-tech querying and analysis without any case-by-case judicial approval").

18. Oral Argument, Smith v. Obama, No. 14-3555 (9th Cir. Dec. 8, 2014). Oral Argument, Klayman v. Obama, No. 14-5004 (D.C. Cir. Nov. 4, 2014); Oral Argument, ACLU v. Clapper, No. 14-42-cv (2d Cir. Sept. 2, 2014).

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

20. *Klayman*, 957 F. Supp. 2d at 37.

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

States, decisions in *United States v. Jones*[22] and *Florida v. Jardines*,[23] which this Article suggests provide guidance for analyzing the bulk telephony metadata collection program under the Fourth Amendment going forward. In Part V, this Article considers the shortcomings of the current Fourth Amendment solutions, from both courts and commentators, to the Fourth Amendment problems high-technology surveillance presents. Part VI incorporates the teachings of *Jones* and *Jardines* into the Court's general Fourth Amendment jurisprudence and sets out a theory of qualitative limits to third-party disclosures in the digital age for courts to apply in testing the constitutionality of programs like the NSA's bulk telephony metadata collection program.

I. THIRD-PARTY DISCLOSURES AND THE FOURTH AMENDMENT

The Fourth Amendment is regarded as "indispensable to the full enjoyment of the rights of personal security, personal liberty, and private property."[24] As a starting point for Fourth Amendment interpretation, "interference with property rights provides a surprisingly helpful guide to the scope of Fourth Amendment protection."[25] Thus, prior to the 1960s, the Supreme Court's "controlling precedent . . . held that the fourth amendment was not applicable unless there was an actual, physical penetration into a constitutionally-protected area."[26] Accordingly, the Court long has recognized that the Fourth Amendment's protections, however indispensable, are not absolute.[27] Among limitations on Fourth Amendment protections, the United States Supreme Court consistently rejects Fourth Amendment claims "using assumption of risk analysis."[28] The Court's third-party disclosure doctrine—a critical limit on the Amendment's protections—is a subset of this assumption of risk

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

23. Florida v. Jardines, 133 S. Ct. 1409 (2013).

24. *See* 3 JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES § 1895 (Fred B. Rothman & Co. 1991) (1833).

25. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 516 (2007).

26. Charles E. Moylan, Jr. & John Sonsteng, *Fourth Amendment Applicability*, 16 WM. MITCHELL L. REV. 209, 221 (1990).

27. *See, e.g.*, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev. 349, 357 (1974) (noting that "the Supreme Court and the lower courts commonly used the concept of a 'constitutionally protected area' to define the scope of the fourth amendment's protection . . . ," but recognizing that the property-based notions of Fourth Amendment protections did not extend to all of a person's property. Thus, "[t]he constitutional protection of houses . . . was not extended to 'the open fields'") (footnotes omitted)).

28. THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION § 3.5.1.1, at 83 (2008).

analysis: "[B]y exposing . . . information . . . to a third person, one *assumes the risk* that the third person will disclose the information . . . to the police . . . ."[29]

The Supreme Court laid the foundation for the development of the third-party disclosure doctrine in 1967 with its decision in *Katz v. United States*.[30] There, the Court shifted the focus of Fourth Amendment protection from property interests to privacy interests.[31] The lasting legacy of *Katz* is the two-pronged test that emerged from Justice John Marshall Harlan II's concurring opinion. Justice Harlan framed the issue in Fourth Amendment cases as determining the scope of the protection "afford[ed] to th[e] people."[32] The answer to this question, said Justice Harlan, depends on a "twofold" inquiry.[33] First, courts must ask whether the person objecting to the government activity "exhibited an actual (subjective) expectation of privacy."[34] If the court finds that the person exhibited an actual expectation of privacy, the court must then ask whether "that . . . expectation [is] one that society is prepared to recognize as 'reasonable.'"[35]

Thus, under Justice Harlan's test, "a person must exhibit an actual subjective expectation of privacy and that expectation must be [objectively reasonable]."[36] If the person's expectations fail either prong of Harlan's test, Fourth Amendment protections do not apply,[37] and "where the fourth amendment is inapplicable, the law does not give a constitutional damn about noncompliance."[38]

Although commentators thought of the pre-*Katz* focus on constitutionally protected places as "awkward and tend[ing] to yield inequitable results,"[39] the "property-based construction of the fourth amendment proved to be remarkably durable," even in the face of an ever-advancing

---

29. *Id*. (emphasis added).
30. Katz v. United States, 389 U.S. 347 (1967).
31. *See, e.g.*, Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint For Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1303 (2002) ("In the late 1960's, the Supreme Court engineered a paradigm shift in Fourth Amendment law: instead of focusing solely on property interests in determining whether or not a 'search' had occurred, the Court broadened the scope of the Amendment's protection to include any activity in which an individual has 'a reasonable expectation of privacy.'" (footnotes omitted)).
32. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
33. *Id*.
34. *Id*.
35. *Id*.
36. CLANCY, *supra* note 28, § 3.3.1, at 60.
37. *Id*.
38. Moylan & Sonsteng, *supra* note 26, at 210.
39. Note, *From Private Places to Personal Privacy: A Post-Katz Study of Fourth American Protection*, 43 N.Y.U. L. REV. 968, 968 (1968).

technological world.[40] *Katz* freed the Fourth Amendment from the bounds of the rigid "constitutionally protected" areas inquiry, but the decision also ushered in a new set of problems for courts in defining the scope of their privacy analysis. While *Katz* "expand[ed] . . . the boundaries of fourth amendment [sic] protection[,] . . . . it offer[ed] neither a comprehensive test of fourth amendment [sic] coverage nor any positive principles by which questions of coverage can be resolved."[41] "The decision seemed to banish to legal limbo much of the judiciary's prior experience with the fourth amendment [sic], and the highly elastic boundaries of the 'reasonable expectation of privacy' test made judicial construction of the amendment quite haphazard."[42] There is agreement that "since *Katz v. United States* the touchstone of [Fourth] Amendment analysis has been the question of whether a person has a 'constitutionally protected reasonable expectation of privacy.'"[43] However, determining what constitutes a "reasonable expectation of privacy" has often proved vexing. Indeed, both the lower courts and the Supreme Court have struggled with "the seemingly indeterminate *Katz* test, and the broad range of factors logically impinging upon it."[44] The struggle for courts has been not only to define when individuals can justifiably—or reasonably—rely on privacy under *Katz*'s first prong, but also to define what types of "police investigative practice[s] . . . threaten[] that sense of security" under *Katz*'s second prong.[45] At bottom, inquiries attempting to define justifiable reliance on privacy inevitably turn on the

---

40. Richard G. Wilkins, *Defining the 'Reasonable Expectation of Privacy': An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077, 1085 (1987) (footnote omitted).

41. Amsterdam, *supra* note 27, at 385; Wilkins, *supra* note 40 at 1088 ("Under *Katz* the fourth amendment applies whenever government activity infringes upon a 'reasonable expectation of privacy;' unfortunately, however, *Katz* itself provides no clear indication how the lower courts are to draw that line.").

42. Wilkins, *supra* note 40, at 1088. Note, however, that in *Florida v. Jardines*, 133 S. Ct. 1409 (2013), and *United States v. Jones*, 132 S. Ct. 945 (2012), the Court emphasized that *Katz* added to the protections of the Fourth Amendments without displacing property rights as a measure by which to gauge Fourth Amendment protections. *See Jardines*, 133 S. Ct. at 1414 ("By reason of our decision in *Katz v. United States* property rights 'are not the sole measure Fourth Amendment violations,'—but though *Katz* may add to the baseline, it does not subtract anything from the Amendment's protections 'when the Government *does* engage in [a] physical intrusion of a constitutionally protected area.'") (alteration in original) (citations omitted)).

43. Oliver v. United States, 466 U.S. 170, 177 (1984) (quoting *Katz*, 389 U.S. at 360 (Harlan, J., concurring)).

44. Wilkins, *supra* note 40, at 1090.

45. *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(d), at 440-45; *see also* Smith v. Maryland, 442 U.S. 735, 740 (1979) ("Consistently with *Katz*, this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action." (citing cases)).

courts' "determin[ation of] what kind of privacy we are *entitled* to expect."[46]

While courts have reached inconsistent results applying *Katz*,[47] the 1970s saw the Court "create[] an exception to Fourth Amendment protections for papers turned over to a third party."[48] Since then, courts uniformly have held that "[i]ndividuals generally lose a reasonable expectation of privacy in their information once they reveal it to third parties."[49] This third-party disclosure exception to the Fourth Amendment's protection of an individual's reasonable expectation of privacy is grounded in the *Katz* majority's recognition that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[50]

The development of the third-party disclosure doctrine is traceable to *United States v. Miller*. There, the Court concluded that depositors have "no legitimate 'expectation of privacy'" in bank records created from checks and deposit slips.[51] In so holding, the Court started from the premise that no protected interests are implicated "unless there is a[] [government] intrusion into a zone of privacy."[52] In considering whether the government seizure of copies of bank records "violate[d] the privacy upon which [the depositor] justifiably relie[d],"[53] the Court cited *Katz* for the proposition that one cannot justifiably rely on the privacy of "'[w]hat a person knowingly exposes to the public.'"[54] Accordingly, the Court "perceived no legitimate 'expectation of privacy'" in the contents of the bank records that third-party banks created from information drawn from checks deposited at the bank.[55] Under this theory, "[t]he depositor takes the risk[] in revealing his affairs to another" and, in doing so, also loses the protection of the Fourth Amendment as to those matters disclosed to third parties.[56]

Just three years later, in *Smith v. Maryland*, the Court reasoned that the holding of *Miller* compelled the conclusion that an individual

---

46. STEPHEN J. SCHULOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 121 (2012).

47. Wilkins, *supra* note 40, at 1090, 1090 n. 56 (noting that "lower courts' sometimes inconsistent application of the [*Katz*] standard is understandable" and citing cases).

48. Alyssa H. DaCunha, Comment, *Txts R Safe 4 2Day:* Quon v. Arch Wireless *and the Fourth Amendment Applied to Text Messages*, 17 GEO. MASON L. REV. 295, 296 (2009).

49. *E.g.*, Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001).

50. Katz v. United States, 389 U.S. 347, 351 (1967).

51. United States v. Miller, 425 U.S. 435, 442 (1976).

52. *Id*. at 440 (internal quotation marks omitted).

53. *Id*. at 442 (internal quotation marks omitted).

54. *Id*. at 442 (quoting *Katz*, 389 U.S. at 351 (1967)) (alteration in original).

55. *Id*.

56. *Miller*, 425 U.S. at 443.

"can claim no legitimate expectation of privacy" in the numbers dialed on a home telephone and "conveyed . . . to the telephone company."[57] The Court concluded that, given the necessary disclosure of the numbers dialed to third-party telephone companies, "telephone subscribers . . . [do not] harbor any general expectation that the numbers they dial will remain secret."[58] Further, even if an individual "harbor[ed] some subjective expectation that the phone numbers . . . dialed would remain private, [that] expectation is not 'one that society is prepared to recognize as 'reasonable.'"[59] This is so, said the Court, because "a person has no legitimate expectation of privacy in information . . . voluntarily turn[ed] over to third parties."[60] In so holding, the Court rejected the defendant's claim that "he demonstrated an expectation of privacy by his conduct . . . since he 'us[ed] the telephone *in his house* to the exclusion of all others.'"[61] The Court held that "the site of the call [was] immaterial for purposes of [Fourth Amendment] analysis."[62] While the fact that the call was made within the confines of the defendant's house may have been material as to the contents of the telephone conversation, the location of the call "could not have been calculated to preserve the privacy of the number he dialed."[63] "Regardless of his location" the defendant had to disclose the number he dialed to the third-party telephone company, placing that information outside the protection of the Fourth Amendment.[64]

II. ELECTRONIC SURVEILLANCE, STATUTORY REGULATION, AND THE NSA'S BULK TELEPHONY METADATA COLLECTION PROGRAM

Miller established that people do not have a reasonable expectation of privacy in records created from information voluntary turned over to third parties during "the normal course of business."[65] *Smith* made it "clear[] [that] one lacks an expectation of privacy in [source and destination information associated with telephone conversations], and law

57. *See Smith*, 442 U.S. at 744.
58. *Id*. at 742-43.
59. *Id*. at 743 (quoting *Katz*, 389 U.S. at 743).
60. *Id*. at 743-44 (citing *Miller*, 425 U.S. at 442-44).
61. *See Smith*, 442 U.S. at 743 (quoting Brief for Petitioner at 6, *Smith*, 442 U.S. 735 (No. 78-5374)) (second alteration in original).
62. *Id.*
63. *Id.*
64. *Id.*
65. Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt of Fourth Amendment Protection*, 11 UCLA J.L. & TECH., Spring 2007, 10 (2007).

enforcement officials need not seek a warrant to acquire it."[66] Thus, together, *Miller* and *Smith* sanctioned broad police investigatory techniques.[67] In the absence of Fourth Amendment protection, Congress has sought to regulate such investigatory practices to balance privacy interests against the needs of law enforcement investigatory efforts outside of the warrant requirement of the Fourth Amendment. One prominent example of statutory regulation of law enforcement investigation is the Foreign Intelligence Surveillance Act ("FISA").[68] Congress enacted FISA in 1978 in "response to intelligence abuse,"[69] "to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes" outside of the warrant requirement of the Fourth Amendment.[70]

On June 5, 2013, *The Guardian* reported the details of a secret Foreign Intelligence Surveillance Court ("FISC") Order authorizing the indiscriminate collection of "the telephone records of millions of US customers of Verizon."[71] This classified Order provided:

> [T]he Custodian of Records shall produce to the National Security Agency . . . on an ongoing and regular basis . . . for the duration of the Order . . . all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.[72]

The Order defines "telephony metadata" as "includ[ing] comprehensive communications routing information, including but not limited

---

66. Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1383 (2004).

67. Lawless, *supra* note, 65 at 9 (under *Miller* and *Smith*, "constitutional privacy interests in information are both bright and binary. It does not matter if the information is exposed for a limited purpose, or in confidence; it matters only whether the individual should know the information was made available to another party").

68. Electronic Surveillance within the United States for Foreign Intelligence Purposes Act, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§1801-1885c).

69. *See* JOHN NORTON MOORE & ROBERT F. TURNER, NATIONAL SECURITY LAW 1072 (2d ed. 2005); *see also* 1 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 3.7, at 105 (2d ed. 2012) [hereinafter 1 KRIS & WILSON] (stating that "[t]he lack of unanimity and the absence of 'systematic analysis' in decisions" reviewing alleged abuses of surveillance in the national security context "were major factors in Congress's decision to regulate electronic surveillance for national security purposes in FISA").

70. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).

71. Greenwald, *Verizon*, *supra* note 2.

72. Secondary Order, *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Production of Tangible Things From Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. D/B/A/ Verizon Bus. Servs., at 1-2, No. BR 13-80 (FISC Apr. 25, 2013).

to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI), etc.), trunk identifier, telephone calling card numbers, and time and duration of the call."[73] Under the Order, "[t]elephony metadata does not include the substantive content of any communication, . . . or the name, address, or financial information of a subscriber or customer."[74] The FISC issued this order pursuant to Section 215 of the USA Patriot Act.

On August 9, 2013, President Barack Obama's administration justified the bulk telephony metadata collection program in a white paper "explain[ing] the Government's legal basis for intelligence collection under which the Federal Bureau of Investigation (FBI) obtains court orders directing certain telecommunications service providers to produce telephony metadata in bulk."[75]

The white paper argued that in the War on Terror the United States faces a significant challenge in "identifying terrorist operatives and networks, particularly those operating within the United States,"[76] and explained the Government has found that analyzing "metadata associated with telephone calls within, to, or from the United States" is a particularly useful tool for trained analysts to root out terrorism-related communications.[77] According to the paper, "[t]he telephony metadata collection program was specifically developed" to enhance the abilities of these analysts and has "help[ed] to close critical intelligence gaps that were highlighted by the September 11, 2001 attacks."[78]

Under the telephony metadata collection program, the FBI works in tandem with the NSA. Once the FBI obtains an order under Section 215 of the USA Patriot Act, the telecommunications service providers subject to the order "produce business records that contain information about communications between telephone numbers."[79] The NSA then "stores and analyzes this information under carefully controlled circumstances."[80]

The NSA may search the database of collected telephony metadata only with an "'identifier,'" referred to as a "'seed,'" which may be a tele-

---

73. *Id.* at 2.
74. *Id.*
75. U.S. DEP'T OF JUSTICE, ADMIN. WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 1 (2013) [hereinafter ADMIN. TELEPHONY METADATA WHITE PAPER], *available at* https://www.aclu.org/files/natsec/nsa/20130816/Section%20215%20-%20Obama%20Administration%20White%20Paper.pdf.
76. *Id.* at 2.
77. *Id.* at 2-3.
78. *Id.* at 3.
79. *Id.*
80. ADMIN. TELEPHONY METADATA WHITE PAPER, *supra* note 75, at 3.

phone number "associated with one of the foreign terrorist organizations that was previously identified to and approved by the [FISC]."[81] In order to use a "seed" to initiate a query of the telephony metadata database, "there must be a 'reasonable, articulable suspicion' that [the] … seed identifier . . . is associated with a particular foreign terrorist organization."[82] After initiation of a database query, NSA analysts obtain certain information that is "responsive" to the query, including the telephone numbers that have been in contact with the "seed" and "the dates, times, and duration of those calls."[83] NSA analysts may then use responsive telephone numbers, referred to as "hops," to commence a query for information responsive to those contacts.[84] This process may continue with the analysts running queries of numbers as far down as the "third 'hop' from the seed telephone number."[85] Through this process of running successive queries of the database, an order issued under the telephony metadata collection program "allows the NSA to retrieve information as many as three" steps removed from the initial "seed" for which there was "reasonable, articulable suspicion" of an association with a terrorist group.[86]

This bulk collection program is subject to Congressional oversight and is monitored by the Department of Justice, the Foreign Intelligence Surveillance Court, and the Intelligence Community.[87] Importantly, however, there is no direct judicial regulation of the program. Prior to initiating a query of the database, one of "twenty-two designated NSA officials" must make a finding that there is "reasonable, articulable suspicion" that the proposed "seed" is indeed "associated with a specific foreign terrorist organization."[88] Further, if a proposed "seed" is believed to belong to a United States citizen, the NSA's Office of General Counsel must approve any findings of "reasonable, articulable suspicion."[89] Of importance here, though, obtaining authorization to query the database *does not* require court approval.[90]

---

81. *Id.*
82. *Id.*
83. *Id.*
84. *Id.* at 4.
85. "The second 'hop' refers to the set of numbers found to be in direct contact with the first 'hop' numbers, and the third 'hop' refers to the numbers found to be in direct contact with the second 'hop' numbers." ADMIN. TELEPHONY METADATA WHITE PAPER, *supra* note 75, at 3-4.
86. *Id.* at 4.
87. *Id.* at 4-5.
88. *Id.* at 5.
89. *Id.*
90. ADMIN. TELEPHONY METADATA WHITE PAPER, *supra* note 75, 5 ("No more than twenty-two designated NSA officials can make a finding that there is 'reasonable, articu-

The Government maintains that the bulk telephony metadata collection program comports with the statutory requirements of Section 215 of the USA Patriot Act and that the program is consistent with the Fourth Amendment to the United States Constitution.[91] For purposes of this article, discussion of the legal justifications for the bulk telephony metadata collection program is limited to the administration's constitutional justifications.

The Government first contends that the orders for production of telephony metadata do not, in themselves, constitute a "search" within the meaning of the Constitution, because, under *Smith*, "participants in telephone calls lack any reasonable expectation of privacy . . . in the telephone numbers dialed."[92] Further, the Government contends that individuals similarly have no reasonable expectation of privacy in the information regarding "the length and time of the calls . . . routing, addressing, or signaling information," because under *Smith* "there is no reasonable expectation of privacy in such information, which is routinely collected by telecommunications services providers for billing and fraud detection purposes."[93]

Even assuming *arguendo* that the bulk telephony metadata collection program constituted a Fourth Amendment "search," the Government argues that the program still would not offend the Fourth Amendment because the "search would satisfy the reasonableness standard that the Supreme Court has established in its cases authorizing the Government to conduct large-scale, but minimally intrusive, suspicionless searches."[94] According to Supreme Court precedent, such a reasonableness inquiry balances the intrusion upon an individual's privacy that the "search" occasions against the public interest that the "search" advances. Here, the Government argues that the minimally invasive collection of telephony metadata is substantially outweighed by the "public interest in the prevention of terrorist attacks."[95] The Government's reasonableness justifications, however, fall beyond the pale of this Article's Fourth Amendment discussion.

---

lable suspicion' that a seed identifier proposed for query is associated with a specific foreign terrorist organization, and NSA's Office of General Counsel must review and approve any such findings for numbers believed to be used by U.S. persons.").

91. *Id.* at 5, 19.
92. *Id.* at 19.
93. *Id.* at 20.
94. *Id.* at 21.
95. ADMIN. TELEPHONY METADATA WHITE PAPER, *supra* note 75, at 21.

III. UNITED STATES DISTRICT COURTS SPLIT ON THE CONSTITUTIONALITY OF BULK TELEPHONY METADATA COLLECTION

Following closely on the heels of the Edward Snowden leaks, United States District Courts began fielding complaints challenging the constitutionality and statutory authorization of the NSA's bulk telephony metadata collection program.[96] On the issue of the program's constitutionality, the United States District Court for the District of Columbia, the United States District Court for the Southern District of New York, and the United States District Court for the District of Idaho have reached conflicting conclusions in *Klayman v. Obama*,[97] *ACLU v. Clapper*,[98] and *Smith v. Obama*,[99] respectively.

A. THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA DISTRICT FINDS BULK TELEPHONY METADATA COLLECTION "LIKELY" UNCONSTITUTIONAL IN *KLAYMAN V. OBAMA*

The day after *The Guardian* reported on the Edward Snowden leaks, plaintiff telecommunication and internet service subscribers filed suit "challenging the constitutionality and statutory authorization" of the bulk telephony metadata collection program.[100] In considering plaintiffs' motion for a preliminary injunction during the pendency of the suit, United States District Judge Richard J. Leon concluded that plaintiffs "demonstrated a substantial likelihood of success on the merits of their Fourth Amendment claim, and that they will suffer irreparable harm absent preliminary injunctive relief," thus entitling them to a preliminary injunction of the bulk telephony metadata collection program.[101]

Judge Leon framed the Fourth Amendment challenge as one alleg-

---

96. *E.g.*, Complaint for Declaratory and Injunctive Relief, ACLU v. Clapper, No. 13-CIV-3994, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013) (No. 13-CIV-3994); Complaint, Klayman v. Obama, 2013 WL 6598728 (D.D.C. Dec. 16, 2013) (No. 1:13-CV-00881); Petition for a Writ of Mandamus and Prohibition, or a Writ of Certiorari, *In re* Electronic Privacy Information Center, No. 13-50 (S. Ct. June 8, 2013), *cert. denied* 134 S. Ct. 638 (2013) (mem.); Complaint for Constitutional and Statutory Violations, Seeking Declaratory and Injunctive Relief, First Unitarian Church of Los Angeles v. NSA, No. CV 13 3287 (N.D. Cal. July 16, 2013); Complaint, Smith v. Obama, No. 2:13-cv-00257 (D. Idaho June 12, 2013).

97. *Klayman*, No. 1:13-CV-00881, 2013 WL 6598728.

98. *Clapper*, No. 13-CIV-3994, 2013 WL 6819708.

99. *Smith*, No. 2:13-cv-00257, 2014 WL 2506421.

100. *Klayman*, No. 1:13-CV-00881, 2013 WL 6598728, at *1.

101. *Id.* at *2.

ing a violation of subjective and reasonable expectations of privacy.[102] Framed in this way, the issue presented was in the familiar form of determining whether plaintiffs held a reasonable expectation of privacy in their telephony metadata that the Government violates by collecting it "along with the metadata of hundreds of millions of other citizens without any particularized suspicion of wrongdoing, retains all of that metadata for five years, and then queries, analyzes, and investigates that data without prior judicial approval of the investigative targets."[103] In addressing this issue, Judge Leon distinguished the bulk telephony metadata collection program from the pen register at issue in *Smith*.[104] Instead, Judge Leon stated that evolution, both in Government surveillance technology and in "citizens' phone habits," have "become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply."[105]

In support of this position, Judge Leon first noted that the scope of data collected under the bulk telephony metadata collection program is vastly different than the collection at issue in *Smith*. Indeed, the pen registers in use in *Smith* had limited recording capabilities and limited scope. Thus, the Supreme Court in *Smith* considered only "forward-looking" data collected over a short time period.[106] However, the bulk telephony metadata collection program "involves the creation and maintenance of a *historical* database containing *five years'* worth of data."[107] Not only is the scope of data collected different, but the time period over which the data is collected has changed. While the "pen register in *Smith* was operational for only a matter of days," the exigency that spawned the bulk telephony collection program—the War on Terror—could very well last for years, if not decades, and "there is the very real prospect that the program will go on for as long as America is combatting terrorism."[108] Indeed, Judge Leon noted, the program could foreseeably go on forever.[109]

Judge Leon then went on to explain that not only had the technology in use changed from *Smith*, but also that the relationship between the Government and the phone companies under the bulk telephony metadata collection program is vastly different from "the relationship between the police and the phone company in *Smith*."[110] Namely, Judge

---

102. *Id.* at *17 ("This case obviously does not involve a physical intrusion, and plaintiffs do not claim otherwise.").
103. *Id.*
104. *Id.* at *18.
105. *Id.*
106. *Klayman*, 2013 WL 6598728, at *19.
107. *Id.*
108. *Id.*
109. *Id.*
110. *Id.*

Leon focused on the fact that in *Smith* third-party telephone companies were merely collecting information for police whereas under the bulk telephony metadata collection program third-party telephone companies have been turning over call detail information daily since May 2006.[111] This difference between the programs was crucial because there is "a meaningful difference between cases in which a third party collects information and then turns it over to law enforcement and cases in which the government and the third party create a formalized policy under which the service provider collects information for law enforcement purposes."[112] Thus, the telephony metadata collection scheme under which service providers indiscriminately collect a vast database of information for law enforcement purposes is meaningfully different than the "one-time, targeted request for data regarding an individual suspect in a criminal investigation" at issue in *Smith*.[113]

Judge Leon also found that the technology at issue in bulk telephony metadata collection is vastly different than the technology at issue in *Smith*. In *Smith*, the Court considered pen registers that were, at the time, able to "collect *one person's* phone records for calls made *after* the pen register was installed and for the *limited purpose* of a small-scale investigation."[114] By contrast, the technology at the Government's disposal today—and in use in the bulk telephony metadata collection program—allows the Government to "collect similar data on *hundreds of millions of people* and retain that data for a five-year period, updating it with new data every day in perpetuity."[115] Such technology "was at best, in 1979, the stuff of science fiction."[116]

Finally, Judge Leon found that the sheer difference in the quality of telephony metadata today distinguished the bulk telephony metadata collection program from the pen register at issue in *Smith*.[117] Not only do almost all United States citizens use mobile connections, the phones they use "have also morphed into multi-purpose devices."[118] Additionally, cell phones follow their users everywhere—where mobile phones are today, there would be no phones when the Court decided *Smith*. Thus, while "the *types* of information at issue . . . are relatively limited," like

---

111. *Id.*

112. *Klayman*, 2013 WL 6598728, at *19 (citation omitted) (citing Ferguson v. Charleston, 532 U.S. 67 (2001)).

113. *Id.*

114. *Id.* at *20 (emphasis added).

115. *Id.* (emphasis added).

116. *Id.*

117. *Id.* at *19 ("I am convinced that the surveillance program now before me is so different from a simple pen register that *Smith* is of little value in assessing whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search.").

118. *Klayman*, 2013 WL 6598728, at *20.

in *Smith*, "the ubiquity of phones has dramatically altered the *quantity* of information that is now available and, *more importantly*, what that information can tell the Government about people's lives."[119] Judge Leon went on to note that the ubiquity of mobile phone use has also changed people's relationship with their phones: "This rapid and monumental shift towards a cell phone-centric culture means that the metadata from each person's phone 'reflects a wealth of detail about her familial, political, professional, religious, and sexual associations,' that could not have been gleaned from a data collection in 1979."[120] Whereas in 1979 the use of a pen register might have revealed a piecemeal picture of a person's life, collection of metadata today "reveal[s] an entire mosaic—a vibrant and constantly updating picture of the person's life."[121] Judge Leon found that "these cultural changes . . . have resulted in a *greater* expectation of privacy and a recognition that society views that expectation as reasonable."[122]

Accordingly, because of the significant changes in technology since *Smith*, Judge Leon found that the collection of telephony metadata likely constituted a Fourth Amendment "search" notwithstanding the fact that plaintiffs disclosed the collected information to a third party.[123] The United States Court of Appeals for the District of Columbia Circuit heard oral argument on the United States' appeal from Judge Leon's order on November 4, 2014.[124]

B. THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK UPHOLDS THE CONSTITUTIONALITY OF BULK TELEPHONY METADATA COLLECTION IN *ACLU V. CLAPPER*

Unlike Judge Leon's extensive Fourth Amendment analysis in *Klayman*, United States District Judge William H. Pauley III gave the Fourth Amendment challenge to the NSA's bulk telephony metadata collection program relatively short shrift in dismissing plaintiffs' complaint in *ACLU v. Clapper*. Relying on *Smith*, Judge Pauley started from the position that "individual[s] ha[ve] no legitimate expectation of privacy in information provided to third parties."[125] In rejecting plaintiffs' invitation to distinguish *Smith* on the basis of the quantity and quality of information disclosed under the bulk telephony metadata col-

119. *Id.*

120. *Id.* (citation omitted) (quoting United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring)).

121. *Id.* at *19.

122. *Id.*

123. *Id.*

124. Oral Argument, Klayman v. Obama, No. 14-5004 (D.C. Cir. Nov. 4, 2014).

125. ACLU v. Clapper, No. 13-CIV-3994, 2013 WL 6819708, at *20 (S.D.N.Y. Dec. 27, 2013).

lection program, Judge Pauley first noted that the NSA can only query that information with "legal justification—subject to rigorous minimization procedures" and that, once queried, the information produced is limited and does not identify the owners of telephone numbers.[126] He then went on to state that "[t]he collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search."[127] Responding directly to Judge Leon's contention that the drastic change in people's relationship with their phones warranted distinguishing *Smith*, Judge Pauley "observe[d] that their relationship with their telecommunications providers has not changed."[128] Unlike Judge Leon, Judge Pauley was not persuaded that the versatility of mobile phones distinguished *Smith*. Indeed, bulk telephony metadata collection implicates only the cellphone's "use as telephones" and "[t]he fact that there are more calls placed does not undermine the Supreme Court's finding that a person has no subjective expectation of privacy in [their] telephony metadata."[129]

Thus, at bottom, Judge Pauley saw no distinction between bulk telephony metadata collection and the use of a pen register at issue in *Smith*.[130] Accordingly, *Smith* controlled Judge Pauley's reasoning and he found that "the NSA's bulk telephony metadata collection program does not violate the Fourth Amendment."[131] The United States Court of Appeals for the Second Circuit heard oral argument in the appeal from Judge Pauley's order on September 2, 2014.[132]

C. THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF IDAHO RELUCTANTLY UPHOLDS THE CONSTITUTIONALITY OF BULK TELEPHONY METADATA COLLECTION IN *SMITH V. OBAMA*

Apparently taking a middle road between Judge Pauley and Judge Leon, United States District Court Chief Judge B. Lynn Winmill upheld the NSA's bulk telephony metadata collection program in the face of a

126. *Id.* at *21.
127. *Id.* at *22.
128. *Id.*
129. *Id.*
130. *See Id.* at *22 ("Importantly, 'what metadata is has not changed over time,' and '[a]s in *Smith*, the *types* of information at issue in this case are relatively limited: [tele]phone numbers dialed, date, time, and the like.'") (alteration in original) (quoting Klayman v. Obama, No. 1:13-CV-0881, 2013 WL 6598728, at *21) (D.D.C. Dec. 16, 2013)).
131. *Clapper*, 2013 WL 6819708, at *22 ("Because *Smith* controls, the NSA's bulk telephony metadata collection program does not violate the Fourth Amendment.").
132. Oral Argument, ACLU v. Clapper, No. 14-42-cv (2d Cir. Sept. 2, 2014).

constitutional challenge, but did so reluctantly.[133] Though noting, as Judge Pauley did, that "*Smith* was not overruled" and, accordingly, controlled the outcome of plaintiff's challenge to the NSA program,[134] Judge Winmill gave credence to plaintiff's Fourth Amendment challenge to the bulk telephony metadata collection program. Citing Judge Leon's opinion approvingly, Judge Winmill opined that the reasoning there "should serve as a template for a Supreme Court opinion" and predicted that "it might yet."[135] Thus, unlike Judge Pauley's outright rejection of a Fourth Amendment challenge to the NSA's bulk telephony metadata collection program, Judge Winmill agreed with Judge Leon's reasoning, but nonetheless concluded he was bound by *Smith*. On December 8, 2014, the United States Court of Appeals for the Ninth Circuit heard oral argument on Smith's appeal from Judge Winmill's order.[136]

IV. RECENT SUPREME COURT CASES SHOW THE WRITING ON THE WALL FOR NSA BULK METADATA COLLECTION

In recent Supreme Court decisions, the Court has struggled both with application of *Katz*'s reasonable expectation of privacy test in light of the significant advances in technology since *Smith* and in light of the cultural shift toward ever-increasing reliance on technology for daily tasks. The Court also has indicated potential limits to its assumption-of-risk analysis, with which the third-party-disclosure doctrine is tied up. This Part will examine those decisions and their implications for the future of the third-party disclosure doctrine.

A. *UNITED STATES V. JONES*[137] CONCURRING OPINIONS INDICATE A POTENTIAL SHIFT IN THE COURT'S THIRD-PARTY DISCLOSURE DOCTRINE

Both Judge Leon and the plaintiffs in *Clapper* relied heavily on Justice Sonya Sotomayor's concurrence in *United States v. Jones*.[138] In that case, the Supreme Court held "that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitute[d] a 'search.'"[139] Writing for the

133. *See* Smith v. Obama, No. 2:13-CV-257, 2014 WL 2506421, at *3-4 (D. Idaho June 3, 2014).
134. *Id.* at *4.
135. *Id.* at *3.
136. Oral Argument, Smith v. Obama, No. 14-3555 (9th Cir. Dec. 8, 2014).
137. United States v. Jones, 132 S. Ct. 945 (2012).
138. Klayman, v. Obama, No. 1:13-CV-0881, 2013 WL 6598728, at *17-18, *20-21 (D.D.C. Dec. 16, 2013); Pl.'s Mem. of Law in Opp'n to Defs.'s Mot. to Dismiss at 27-29, ACLU v. Clapper, No. 13-CIV-3994, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013).
139. *Jones*, 132 S. Ct. at 949 (footnote omitted).

Court, Justice Antonin Scalia, harkening back to *Olmstead v. United States*,[140] focused on government trespass upon private property to find that the government action at issue constituted a "search," rather than focusing on any inquiry into the defendant's expectations of privacy.[141] Indeed, Justice Scalia opined that deciding the case at hand based on a *Katz* expectation of privacy analysis would "needlessly lead[] [the Court] into 'particularly vexing problems."[142] However, five Justices did analyze the Government's GPS surveillance under the *Katz* rubric and indicated that the Court might be ready to reexamine its third-party disclosure doctrine.[143]

Notably, Justice Sotomayor's concurrence expressly raised the specter that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[144] In doing so, Justice Sotomayor opined that the third-party disclosure doctrine was no longer a good fit for the advancing "digital age."[145] Today, she explained, "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[146] In light of the necessities of such disclosures in the digital age, Justice Sotomayor "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."[147]

Justice Alito, writing for Justices Ginsburg, Breyer, and Kagan, went even further than Justice Sotomayor and applied a full-blown *Katz* reasonable expectation of privacy analysis to the GPS monitoring

---

140. *Olmstead* was the Court's leading precedent on the trespass-based inquiry to the Fourth Amendment before *Katz*. Olmstead v. United States, 277 U.S. 438 (1928).

141. *Jones*, 132 S. Ct.at 950 (rejecting the Government's argument that "no search occurred . . . since Jones had no 'reasonable expectation of privacy' in the area of the Jeep accessed by Government agents . . . and in the locations of the Jeep on the public roads, which were visible to all . . . , because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. . . . [F]or most of our history the Fourth Amendment was understood to embody a particular concern for government *trespass* upon the areas . . . it enumerates." (fourth alteration in original) (emphasis added) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001))).

142. *Id.* at 953 .

143. *Id.* at 954-56 (Sotomayor, J., concurring); *Id.* at 958 (Alito, J., concurring) ("I would analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.").

144. *Id.* at 957 (Sotomayor, J., concurring).

145. *Id.* (Sotomayor, J., concurring).

146. *Id.* (Sotomayor, J., concurring).

147. *Jones*, 132 S. Ct. at 957 (emphasis added) (Sotomayor, J., concurring).

at issue.[148] In doing so, Justice Alito noted that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable."[149] However, where short-term monitoring lapses into "secretly monitor[ing] and catalogu[ing] every single movement of an individual's car for a very long period of time" the Government surveillance "impinges on expectations of privacy" and, thus, implicates the Fourth Amendment.[150] While not establishing the line at which point Government surveillance triggers Fourth Amendment protections, Justice Alito wrote that tracking Jones's vehicle continuously for four weeks clearly crossed that line.[151] Justice Alito reasoned that advancing technology was changing society's expectations of privacy and "[d]ramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes."[152]

Surely, some people may readily accept the convenience that advancing technology provides and view decreased privacy as an "expense" in a sort of "tradeoff" for the benefits of technology.[153] Justice Alito explained, it may be that as this intrusion on privacy increases, "concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions."[154] However, in the absence of such legislation, it is for the courts "to apply existing Fourth Amendment doctrine" to the facts presented in cases involving use of advanced technology to conduct "searches."[155]

B. *FLORIDA V. JARDINES* TURNS ON A LIMITED LICENSE THEORY

In *Florida v. Jardines*,[156] the Court found that a dog sniff conducted on the defendant's front porch constituted a Fourth Amendment "search."[157] The majority, per Justice Scalia, did so without considering whether the dog sniff outside of the defendant's home infringed on his reasonable expectation of privacy.[158] Instead, the Court framed the is-

148. *See Id.* at 958 (Alito, J., concurring) ("I would analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.").
149. *Id.* at 964. (Alito, J., concurring).
150. *Id.* (Alito, J., concurring).
151. *Id.* (Alito, J., concurring).
152. *Id.* at 962 (Alito, J., concurring).
153. Jones, 132 S. Ct. at 962 (Alito, J., concurring).
154. *Id.*(Alito, J., concurring).
155. *Id.*(Alito, J., concurring).
156. Florida v. Jardines, 133 S. Ct. 1409 (2013).
157. *Id.* at 1417-18.
158. *Id.* at 1417.

sue as whether, by bringing a trained narcotics dog on to defendant's property, the Government impermissibly physically intruded into the curtilage of his home.[159] In analyzing the question thus framed, the Court recognized the "implicit license [that] typically permits the visitor to approach the home by the front path, knock promptly, wait briefly to be received, and then (absent invitation to linger longer) leave."[160] Accordingly, "a police officer not armed with a warrant may approach a home and knock, precisely because that is 'no more than any private citizen might do.'"[161] However, the Court went on to explain, bringing a trained police dog along "in hopes of discovering incriminating evidence is something" beyond what the implied license permits.[162] Thus, because "the background social norms that invite a visitor to the front door do not invite him there to conduct a search," the officers violated the scope of the implied license and were thus trespassing on defendant's property[163]—customary licenses in favor of the public at large do not permit police officers leave to conduct a law enforcement investigation. Indeed, "[t]he scope of a license—express or implied—is limited not only to a particular area but also to a *specific purpose*."[164] As such, the case was "a straightforward one" for the Court in that the officers "gathered . . . information by physically entering and occupying the area" without explicit or implicit leave from the homeowner in violation of core Fourth Amendment tenets.[165]

While agreeing with the property analysis of the majority, Justice Elena Kagan, writing for Justices Ginsburg and Sotomayor, "wr[o]te separately to note that [she] could just as happily decided it by looking to Jardines' privacy interests."[166] In doing so, Justice Kagan indicated a possible continued change in thinking regarding expectations of privacy. Justice Kagan suggested, as did the majority, that allowing the Government to thwart Fourth Amendment protections by taking advantage of limited licenses would frustrate the "practical value" of Fourth Amendment rights.[167]

---

159. *Id.* at 1416-17.
160. *Id.* at 1415.
161. *Id.* at 1416 (quoting Kentucky v. King, 131 S. Ct. 1849, 1862 (2011)).
162. *Jardines*, 133 S. Ct. at 1416 (quoting *King*, 131 S. Ct. at 1862).
163. *Id.*
164. *Id.* (emphasis added).
165. *Id.* at 1414.
166. *Id.* at 1418 (Kagan, J., concurring).
167. *Id.* at 1418 (Kagan, J., concurring) (insisting on the maintenance of one's right "to retreat into his own home and there be free from unreasonable governmental intrusion . . . by preventing police officers from standing in an adjacent space and trawl[ing] for evidence with impunity." (second alteration in original) (internal quotation marks omitted)).

V. HOW *JONES* AND *JARDINES* GUIDE ANALYSIS OF THE NSA BULK TELEPHONY COLLECTION PROGRAM

Since *Jones*, there has been wide discussion among commentators about the case's potential effect on high technology surveillance and the Fourth Amendment.[168] While much of the commentary has focused on the significance of Justice Scalia's purported return to "a trespass-first rule,"[169] other commentary has discussed the privacy-based Fourth Amendment implications of "five justices, in two separate concurring opinions [in *Jones*], . . . suggest[ing] that an important constitutional line is crossed—and the constraints of the Fourth Amendment are triggered—when public surveillance becomes too intense or prolonged."[170] For instance, Justice Alito's concurrence has been lauded as "a new *Katz* test" under which "police conduct is a search when it 'involve[s] a degree of intrusion that a reasonable person would not have anticipated' in that 'particular case.'"[171]

As discussed above,[172] when faced with the issue of the constitutionality of the NSA's bulk metadata collection program in the post-*Jones* world, three United States District Courts have disagreed as to

---

168. *See generally, e.g.*, Kevin Emas & Tamara Pallas, United States v. Jones*: Does Katz Still Have Nine Lives?*, 24 ST. THOMAS L. REV. 116, 117 (2012) ("[E]xplor[ing] the Court's recent retreat from the two-part *Katz* test, and [the] unexpected shift in the considerations the Court declared it will primarily rely upon when evaluating whether a Fourth Amendment search occurred."); *see also* Erica Goldberg, *How* United States v. Jones *Can Restore Our Faith in the Fourth Amendment*, 110 MICH. L. REV. FIRST IMPRESSIONS 62, 62 (2011) ("*Jones* should restore our faith in the Fourth Amendment not necessarily because it is more protective of Fourth Amendment rights, but because it gives the Justices a more concrete framework to determine whether the government has executed a search. Because *Jones* has supplemented the reasonableness inquiry with a physical trespass test, the determination of whether government action constitutes a search can be based on objective factors. Over time, this should make the results of Fourth Amendment cases more predictable and defensible and perhaps reduce much of the cynicism surrounding Fourth Amendment jurisprudence.").

169. *E.g.*, Arnold H. Loewy, United States v. Jones*, Return to Trespass—Good News or Bad*, 82 MISS. L.J. 879, 884 (2013) (arguing that under *Jones* "first we look to see if there was a trespass to a person, paper, house, or effect. If the answer is, 'Yes,' and the trespass was for the purpose of finding evidence, then there is a search, and we do not go to the *Katz* analysis" and stating that "[w]hile the trespass in *Jones* may seem trivial, relative to the harm done to privacy by monitoring, there nevertheless was a trespass[] [a]nd, at least now, it is clear that once there is a trespass, the amorphous privacy question does not even have to be reached").

170. Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 26 (2013) (footnote omitted).

171. Jonathan Siegel & Kate Hadley, Jones's *Second Majority Opinion: Justice Alito's Concurrence and The New* Katz *Test*, 31 YALE L. & POL'Y REV. INTER ALIA 1, 2 (2012) (alteration in original) (quoting United States v. Jones, 132 S. Ct. 935, 964 (Alito, J., concurring)).

172. *See supra* Part III.

what, if any, effect *Jones* has had on the third-party disclosure doctrine in a high-tech world. On the one hand, Judge Leon relied heavily on Justice Sotomayor's concurrence in *Jones* to distinguish the NSA's collection program from *Smith* in *Klayman*.[173] On the other hand, Judges Pauley and Winmill flatly rejected the conclusion that *Jones* controlled, with Judge Pauley explaining that plaintiff's "reliance on the concurring opinions in *Jones* [is] misplaced," because "the Supreme Court did not overrule *Smith*" in *Jones* and "[i]nferior courts are bound by that precedent."[174]

This Article does not disagree with Judge Pauley's and Judge Winmill's conclusion that *Jones* did not overrule *Smith* and his contention that *Smith* remains very much good law. However, this Article agrees with Judge Leon's view that the facts of *Smith* are distinguishable from those at issue in the NSA bulk telephony metadata collection cases and argues that today's technology warrants a different view of *Smith* and the third-party disclosure doctrine. However, as this Part demonstrates, the analysis of third-party disclosures that is most faithful to the Court's Fourth Amendment jurisprudence is different than that employed by Judge Leon. Whereas Judge Leon focused on what has been called "quantitative privacy" in order to distinguish *Smith*,[175] this Article argues that expectations of privacy are better informed by asking what limits to a disclosure an individual expects *ex ante* when, say, dialing a phone number.

To that end, Section A below discusses the right of quantitative privacy and Judge Leon's application of the theory of quantitative privacy. Section B then discusses the key doctrinal challenges to implementing a doctrine based solely on quantitative privacy and why such a theory does not fit within the Court's current third-party disclosure doctrine.

A. THE "MOSAIC THEORY" OF THE FOURTH AMENDMENT AND JUDGE LEON'S APPLICATION OF A TECHNOLOGY-FOCUSED RIGHT TO QUANTITATIVE PRIVACY

In *Klayman*,[176] Judge Leon focused extensively on the scope of the NSA's bulk telephony metadata collection in distinguishing *Smith* and

---

173. *See supra* Part III.A.

174. ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013); Smith v. Jones, No. 2:13-CV-257, 2014 WL 2506421, at *4 (D. Idaho June 3, 2014).

175. For an in depth discussion of "quantitative privacy," see David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013) [hereinafter Gray & Citron, *Quantitative Privacy*].

176. For an in-depth discussion, see *supra* Part III.A.

concluding that "it is significantly likely that" the NSA's program violates phone users' reasonable expectations of privacy.[177] Judge Leon signaled his reliance, though not expressly, on the idea of a right to quantitative privacy by relying on Justice Alito and Justice Sotomayor's concurring opinions in *Jones* for the proposition that while "short-range, short-term" surveillance is consistent with the Fourth Amendment, the longer in duration and broader in scope that surveillance becomes the more it impinges on reasonable expectations of privacy.[178] Thus, on the specific facts presented by the NSA bulk telephony metadata collection program, Judge Leon held that the breadth of the collection along with the duration for which the NSA stored the collected data warranted a finding that the plaintiffs' Fourth Amendment claim was likely to succeed on the merits.[179]

In this sense, Judge Leon's opinion tracks closely with how the United States Court of Appeals for the District of Columbia treated the GPS monitoring at issue in *Jones* in its opinion in *United States v. Maynard*.[180] Professor Orin S. Kerr has termed this approach to a quantitative privacy the "'mosaic theory' of the Fourth Amendment."[181] "Under the mosaic theory, searches can be analyzed as a collective sequence of steps rather than as individual steps."[182] Thus, while individual police actions taken during the course of an investigation may not implicate the Fourth Amendment, "the mosaic can count as a collective Fourth Amendment search" when viewed in its entirety.[183] According to Judge Leon, although turning over telephony metadata in isolation implicates no Fourth Amendment concerns, the cumulative effect of the NSA collection program infringed on reasonable expectations of privacy.[184]

In this way, the "mosaic theory" serves as a sort of a Fourth Amendment stopgap response to technology that is out—pacing the Court's current Fourth Amendment jurisprudence. Professor Kerr points to such stopgaps, like the "mosaic theory," as evidence of "the principle of equilibrium-adjustment."[185] According to Kerr,

---

177. Klayman v. Obama, No. 1:13-CV-0881, 2013 WL 6598728, at *22 (D.D.C. Dec. 16, 2013).

178. *Id*. at *18.

179. *Id.* at *22.

180. United States v. Maynard, 615 F.3d 544, 562-65 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

181. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313, 313 n.5 (2012) [hereinafter Kerr, *Mosaic*].

182. *Id.* at 313.

183. *Id*.

184. *See* Klayman v. Obama, No. 1:13-CV-0881, 2013 WL 6598728 at *22 (D.D.C. Dec. 16, 2013).

185. *See* Kerr, *Mosaic*, *supra* note 181, at 345.

"[e]quilibrium-adjustment is a judicial response to technology and social practice. When new tools and new practices threaten to expand or contract police power in a significant way courts adjust the level of Fourth Amendment protection to try to restore the prior equilibrium [between the State and the citizen]."[186] Thus, in an age where technology enables the government to quickly gather information, aggregate that information, and store it indefinitely in order to analyze later, "[t]he mosaic theory attempts to restore the balance of power by disabling the government's ability to rely on what computerization enables."[187]

However noble the end of the "mosaic theory" is, though, critics of the approach have called the means used in pursuit of that end simply too revolutionary to take hold as the Court's polestar in addressing Fourth Amendment questions. Namely, say the critics, "adopting a mosaic approach to the Fourth Amendment may require abandoning or dramatically altering two important lines of Fourth Amendment law: the public observation doctrine and the third party doctrine."[188] In addition to doctrinal concerns, critics also outline "serious practical concerns that . . . should urge us to caution before adopting the mosaic theory of Fourth Amendment privacy."[189] For instance, Professor Kerr argues that the mosaic theory provides little guidance "explain[ing] how conduct should be grouped to assess whether the collective whole crosses the mosaic line," leaving courts to arbitrarily draw lines.[190]

In light of the critiques of the mosaic theory from scholars and judges alike,[191] defenders of the idea of a right to quantitative privacy and of further adapting Fourth Amendment jurisprudence to today's technological age "argue . . . that Fourth Amendment interests in quan-

---

186. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

187. Kerr, *Mosaic*, *supra* note 181, at 345.

188. *E.g.*, David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J. L. & TECH. 381, 402 (2013).

189. *Id.* at 409.

190. *See* Kerr, *Mosaic*, *supra* note 181, at 329.

191. Justice Scalia expressed his skepticism of the mosaic approach to the Fourth Amendment in his opinion for the Court in *United States v. Jones*. There, Justice Scalia responded to the concurring Justices' reliance on quantitative privacy. United States v. Jones, 132 S. Ct. 945, 953-54 (2012). In doing so, Justice Scalia argued "the concurrence's insistence on the exclusivity of the *Katz* test . . . needlessly leads us into 'particularly vexing problems.'" *Id*. at 953. "The concurrence posits that 'relatively short-term monitoring of a person's movements on public streets' is okay, but that 'the use of longer term GPS monitoring in investigations of *most offenses*' is no good." *Id.* at 954. Indeed, as Justice Scalia's argument goes, the concurrence fails to explain "why a 4-week investigation is 'surely' too long." *Id.* In closing, Justice Scalia challenges this line drawing, asking "What of a 2-day monitoring . . . ? Or of a 6-month monitoring . . . ?" *Id.*

titative privacy demand that we focus on *how* information is gathered . . . [r]ather than asking *how much* information is gathered in a particular case."[192] As such, those defenders of Fourth Amendment protection for quantitative rights of privacy seek to provide guidance for court line drawing. Accordingly, Professors David Gray and Danielle Citron persuasively argue:

> [T]he threshold Fourth Amendment question should be whether the *technology* has the capacity to facilitate broad and indiscriminate surveillance that intrudes upon reasonable expectations of quantitative privacy by raising the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of law enforcement officers or other government agents.[193]

In so arguing, Gray and Citron posit that "[t]he concerns about broad programs of indiscriminate search that drove us to adopt the Fourth Amendment in 1791 are raised anew with law enforcement's unfettered access to contemporary surveillance technologies."[194] Thus, the test they set forth focuses on the "investigative technique or technology" used rather than engaging "on a case-by-case . . . assess[ment of] the quality and quantity of information about a suspect gathered in the course of a specific investigation," as required under the mosaic theory.[195] Thus, when a citizen challenges a government investigatory technique under Gray and Citron's test, a "court would need to consider . . . : (1) the inherent scope of a technology's surveillance capabilities, be they narrow or broad; (2) the technology's scale and scalability; and (3) the costs associated with deploying and using the technology."[196] If, after considering these factors,

> a court finds that a challenged technology is capable of broad and indiscriminate surveillance by its nature, or is sufficiently inexpensive and scalable so as to present no practical barrier against its broad and indiscriminate use, then granting law enforcement unfettered access to that technology would violate reasonable expectations of quantitative privacy.[197]

With Gray and Citron's test in mind, one can read Judge Leon's opinion in *Klayman v. Obama* not only as relying on notions of quantitative rights of privacy, but also as an application of a technology-focused right to quantitative privacy. Similar to Gray and Citron, Judge Leon framed the Fourth Amendment issue as:

---

192. Gray & Citron, *Quantitative Privacy*, *supra* note 175, at 71 (emphasis added).
193. *Id.* at 71-72.
194. *Id.* at 99.
195. *Id.* at 101.
196. *Id.* at 102.
197. *Id.*

> whether plaintiffs have a reasonable expectation of privacy that is violated when the Government indiscriminately collects their telephony metadata . . . without any particularized suspicion of wrongdoing, retains all of that data for five years, and then queries, analyzes, and investigates that data without prior judicial approval of the investigative targets.[198]

In distinguishing *Maryland v. Smith*, Judge Leon concluded that "[t]he question before [him was] *not* the same question that the Supreme Court confronted in *Smith*."[199] Indeed, said Judge Leon, "the circumstances addressed in [*Smith* are] a far cry from the issue in [*Klayman*]."[200] Instead, like Gray and Citron advocate, Judge Leon asked, among other things, when do "the evolutions in the Government's surveillance capabilities . . . become so thorough unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply?"[201] Significantly to Judge Leon in distinguishing *Smith*, "the almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979."[202] Further, "*and most importantly*, not only is the Government's ability to collect, store, and analyze phone data greater now . . . , but the nature and quantity of the information contained in people's telephony metadata is much greater, as well."[203] Thus, tracking closely with the analysis Gray and Citron offer, Judge Leon found that "the *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many distinctions between them that [he] c[ould not] possibly navigate these uncharted Fourth Amendment waters using as [his] North Star a case that predates the rise of cell phones."[204] Rather, when the time comes to decide the Fourth Amendment issue on the merits, Judge Leon found that scope and scale of the surveillance of the NSA bulk telephony metadata collection program made it "significantly likely" that he would find a violation of the plaintiffs' reasonable expectation of privacy.[205]

B. DOCTRINAL SHORTCOMINGS OF A TECHNOLOGY-FOCUSED RIGHT TO

198. Klayman v. Obama, No. 1:13-CV-0881, 2013 WL 6598728, at *17 (D.D.C. Dec. 16, 2013).
199. *Id.* at *18.
200. *Id.*
201. *Id.*
202. *Id.* at *20.
203. *Id.*
204. *Klayman*, 2013 WL 6598728, at *22.
205. *See Id.*

QUANTITATIVE PRIVACY

In *ACLU v. Clapper*, Judge Pauley expressly rejected the ACLU's claim based on notions of quantitative rights to privacy.[206] Judge Pauley stated that "[t]he collection of breathtaking amounts of information *unprotected* by the Fourth Amendment does not transform that sweep into a Fourth Amendment search."[207] Accordingly, finding advancement of a claim predicated on a purported right to quantitative privacy a Fourth Amendment a bridge too far, Judge Pauley concluded that *Smith* controlled and "[i]nferior courts are bound by that precedent."[208]

Thus, Judge Pauley's opinion evinces a clear shortcoming of Professors Gray and Citron's technology-focused right to quantitative privacy—specifically, the idea that a technology implicates the Fourth Amendment if the "challenged technology is capable of broad and indiscriminate surveillance by its nature, or is sufficiently inexpensive and scalable so as to present no practical barrier against its broad and indiscriminate use."[209]

Gray and Citron principally rely on *United States v. Knotts*[210] and *Kyllo v. United States*[211] to support the proposition that "courts have . . . appl[ied] the Fourth Amendment's reasonableness standards" to limit the use of "emerging technologies capable of amassing large quantities of information . . . [that] raise[] the specter of a surveillance state."[212] Specifically, Gray and Citron argue that *United States v. Knotts* "indicated that 'dragnet type law enforcement practices' might threaten broadly held privacy expectations."[213] Additionally, they observe that "[t]he technological capacity to effect pervasive surveillance was . . . at issue in *United States v. Kyllo*" and contend that "Justice Scalia emphasized that the court must not 'permit police technology to erode the privacy guaranteed by the Fourth Amendment,' including existing technologies and 'more sophisticated systems that are already in use or in development.'"[214]

This view of *Kyllo* and *Knotts*, however, simply reads too much into those decisions. For instance, at issue in *Knotts* was the use of "[a] beeper . . . which emit[tted] periodic signals that c[ould] be picked up by a radio receiver" to track the defendant from "Minneapolis, Minnesota

206. *See* ACLU v. Clapper, 959 F. Supp. 2d 724, 750 (S.D.N.Y. 2013).
207. *Id.* at 752.
208. *See Id.*
209. Gray & Citron, *Quantitative Privacy*, *supra* note 175, at 101.
210. United States v. Knotts, 460 U.S. 276 (1983).
211. Kyllo v. United States, 533 U.S. 27 (2001).
212. Gray & Citron, *Quantitative Privacy*, *supra* note 175, at 104-05.
213. *Id.* at 105 (quoting *Knotts*, 460 U.S. at 284).
214. *Id.* (footnotes omitted) (quoting *Kyllo*, 533 U.S. at 34, 36).

to [defendant's] secluded cabin near Shell Lake, Wisconsin."[215] The Supreme Court granted certiorari after "[a] divided panel of the United States Court of Appeals for the Eighth Circuit reversed [defendant's] conviction, finding that the monitoring of the beeper was prohibited by the Fourth Amendment because its use had violated [defendant's] reasonable expectation of privacy."[216] In reversing the Eighth Circuit, then-Justice William Rehnquist, writing for the Court, classified the surveillance at issue as "principally . . . the following of an automobile on public streets and highways."[217] The Court stated, "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[218] Even though the use of the use of a beeper allowed law enforcement officials to follow the defendant with more efficacy, that "d[id] not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[219]

As Gray and Citron note, Justice Rehnquist did address the defendant's argument that the result of upholding the use of the beeper in this case "would be that 'twenty-four hour surveillance of this country will be possible, without judicial knowledge or supervision."[220] However, rather than agreeing with the proposition that some form of quantitative view of privacy would change the result, Rehnquist expressly reserved judgment on the issue, stating that "if such dragnet type law enforcement practices as respondent envisions should eventually occur, there *will be time enough then* to determine whether different constitutional principles may be applicable."[221]

Despite the rapid advance of technology and capabilities of government surveillance, the day warranting application of different constitutional principles to the use of high-technology surveillance has not yet come for the Court. In *United States v. Jones*, Justice Scalia, writing for the Court, considered arguments based on *Knotts* and reaffirmed his commitment to the precedent in light of current technology.[222] However,

---

215. *Knotts*, 460 U.S. at 277.
216. *Id.* at 279-80 (emphasis added).
217. *Id.* at 281.
218. *Id.*
219. *Id.* at 282.
220. *Id.* at 283-284.
221. *Knotts*, 460 U.S. at 284 (emphasis added).
222. United States v. Jones, 132 S. Ct. 945, 953-54 (2012) ("The Court to date has not deviated from the understanding that mere visual observation does not constitute a search."). Like in *Knotts*, Justice Scalia punted on the issue of reasonable expectations of privacy, stating, "[i]t may be that achieving the same result [as constant human surveillance] through electronic means, without an accompanying trespass, is an unconstitution-

the concern expressed in *Knotts* regarding "dragnet type law enforcement practices" seems to be directed not at law enforcement practices capable of aggregating a large quantity of information, but rather at twenty-four hour surveillance that would reveal information that the Fourth Amendment expressly protects. Thus, in *Knotts* the Court was not concerned that the technology allowed for constant tracking, but rather it was significant to the Court that the surveillance did not infringe on "the traditional expectation of privacy *within* a dwelling place."[223] To be sure, had visual surveillance not failed, officers could have observed the car carrying the barrel of contraband leave the public highway and arrive at the cabin. Accordingly, the use of the beeper to accomplish the same end was permissible, because "there [was] no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin."[224]

Kyllo supports this view of Fourth Amendment analysis in light of emerging technology, as the decision there turned on recognized protected privacy rather than notions quantitative rights to privacy. In *Kyllo*, the Court considered "whether the use of a thermal-imaging device aimed at a private home from a street to detect relative amounts of heat within the home constitutes a 'search' within the meaning of the Fourth Amendment."[225]

Thus, *Kyllo* represented another iteration of the Court's jurisprudence analyzing use of enhanced surveillance technology. Before considering the issue so presented in *Kyllo*, the Court had reserved judgment, as it did in *Knotts*, on just how and when such technologically enhanced surveillance might implicate the Fourth Amendment in *Dow Chemical Co. v. United States*,[226] considering whether aerial surveillance of a "2,000 acre plant complex without a warrant was a . . . search under the Fourth Amendment.[227] However, important to the Court in

---

al invasion of privacy, but the present case does not require us to answer that question." *Id.* at 954. However, the fact that the Court could not agree on a proper standard by which to determine such expectations of privacy when the issue seemed to be squarely teed up for it is telling, strongly suggesting that the Court likely is hesitant to embrace the idea of a quantitative right to privacy fully.

223. *Knotts*, 460 U.S. at 282 (emphasis added).

224. *Id.* at 285.

225. Kyllo v. United States, 533 U.S. 27, 29 (2001).

226. Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

227. *Id.* at 229, 238-39 ("It may well be, as the Government concedes, that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed. But the photographs here are not so revealing of intimate details as to raise constitutional concerns. Although they undoubtedly give the EPA more detailed information than naked-eye views, they remain limited to an outline of the facility's buildings and equipment.").

Dow Chemical was the fact that the photographed areas were "*not* an area immediately adjacent to a private home, where privacy expectations are most heightened. Nor [was] this an area where Dow ha[d] made any effort to protect against aerial surveillance."[228]

In confronting the thorny issue of technology's effect on expectations of privacy yet again in *Kyllo*, the Court framed the threshold question as "what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[229] Writing for the Court, Justice Scalia held that "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[230] As Gray and Citron note, Justice Scalia focused on preventing "police technology [from] erod[ing] the privacy guaranteed by the Fourth Amendment."[231] However, unlike Gray and Citron who argue that *Kyllo* tracks a "familiar doctrinal path, invoking the Fourth Amendment to guard against indiscriminate intrusions that compromise 'power to control what others can come to know' about them,"[232] Justice Scalia's rationale appears much more limited. Instead, Justice Scalia drew a bright and "'a firm line at the entrance to the house'" over which government surveillance could not cross.[233] Far from embracing notions of quantitative rights of privacy, Justice Scalia declared that "[t]he Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."[234] In *Jardines*, Justice Scalia further illustrated the Fourth Amendment underpinnings of *Knotts* and *Kyllo* by drawing a line at the threshold of the door past which law enforcement could not cross through the use of sensory-enhancing equipment—e.g., a trained drug dog.[235]

Accordingly, instead of laying the foundation for the recognition of a quantitative right of privacy implicated when advancing technology raises the specter of the surveillance state as Professors Gray and Cit-

---

228. *Id.* at 237 n. 4.
229. *Kyllo*, 533 U.S. at 34.
230. *Id.* at 40.
231. *Id.* at 35.
232. Gray & Citron, *Quantitative Privacy*, *supra* note 175, at 105.
233. *Kyllo*, 533 U.S. at 40 (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).
234. *Id.* at 37.
235. *See* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) ("[W]hen it comes to the Fourth Amendment, the home is first among equals. At the Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreasonable government intrusion.' This right would be of little practical value if the State's agents could stand in a home's porch or side garden and trawl for evidence with impunity.") (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)) (citation omitted)).

ron argue, *Knotts* and *Kyllo* stand for the rather unremarkable proposition that a firm, bright line at the entrance of one's home limits the permissible reach of government technologically-enhanced surveillance. As such, Judge Pauley's admonition that "[t]he collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search" appears to embody a better understanding of the cases relied on by Gray and Citron.[236] The focus of the inquiry for Fourth Amendment purposes is not the quantity or the quality of the information that high-technology surveillance reveals, but rather it is whether access to that information violates "the privacy guaranteed by the Fourth Amendment."[237] Accordingly, before engaging in Gray and Citron's technology-focused inquiry, courts must identify a protected interest that the Fourth Amendment recognizes and that the government surveillance infringes on.

VI. EXAMINING THE SCOPE OF THIRD-PARTY DISCLOSURES: QUALITATIVE LIMITS ON THE THIRD-PARTY DISCLOSURE DOCTRINE IN A TECHNOLOGICAL AGE

All of this is not to say that this Article disagrees with notions of quantitative rights of privacy. Rather, it is meant simply to refute arguments that individual expectations of privacy should *turn* on the type of technology used to gather otherwise unprotected information. This does not mean, however, that the type of technology used to gather information is irrelevant. Indeed, the Court has indicated that technology-enhanced surveillance will infringe on Fourth Amendment protections when such "technology . . . erode[s] the privacy guaranteed by the Fourth Amendment."[238] But where such technology does not intrude on traditionally guaranteed protections of the Fourth Amendment, the mere fact that the technology enhances law enforcement capability to gather evidence is of no moment as far as the Fourth Amendment is concerned.[239] Nonetheless, as Professors Gray and Citron correctly note, the "concurring opinions [in *Jones*] indicate that at least five justices have serious concerns about law enforcement's growing surveillance ca-

236. ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013).

237. *Kyllo*, 533 U.S. at 35.

238. *Id.* at 34.

239. *Cf.* Dow Chem. Co. v. United States, 476 U.S. 227, 238-39 (1986) ("The mere fact that human vision is enhanced somewhat . . . does not give rise to constitutional problems. An electronic device to penetrate walls or windows so as to hear and record confidential discussions . . . would raise very different and far more serious questions."); United States v. Knotts, 460 U.S. 276, 284 (1983) ("Insofar as respondent's complaint appears to be simply that scientific devices such as the beeper enabled the police to be more effective in detecting crime, it simply has no constitutional foundation. We have never equated police efficiency with unconstitutionality.").

pabilities."[240] The question this Part seeks to answer is how to address those concurring Justices' concerns.

This Article argues that the question to ask for Fourth Amendment purposes is, *ex ante*, what people's expectations are regarding their privacy in the digital age. Justice Sotomayor framed the question as applied to the facts in *Jones*: "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[241] Like Gray and Citron's approach, Justice Sotomayor's approach recognizes that the third-party disclosure rule, in its current form, "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."[242] However, unlike Gray and Citron's technology-focused test, Justice Sotomayor's test remains faithful to what Professor Orin S. Kerr identifies as "the sequential approach" to the Fourth Amendment.[243] Under this approach "courts take a snapshot of the act and assess it in isolation."[244] Thus, the Fourth Amendment analysis "requires a frame-by-frame dissection of the scene,"[245] asking first whether there has been an infringement of one's reasonable expectation of privacy.[246]

Accordingly, this Part argues that courts should analyze questions presented by the NSA bulk telephony metadata collection program and other similar surveillance schemes under a traditional, sequential Fourth Amendment rubric. This test first asks, *ex ante*, what telephone users' reasonable expectations of privacy are when using their phones in today's digital age, thus, establishing a qualitative limit on third-party disclosures. Once the court identifies this limit, the court should then proceed to an analysis similar to the test that Professors Gray and Citron offer, asking whether the government surveillance technology in question allows for the discovery information beyond what individual phone users knowingly disclosed to third parties that would otherwise be unknowable. If it has, then the surveillance is a Fourth Amendment "search."

---

240. Gray & Citron, *Quantitative Privacy*, *supra* note 175, at 68.
241. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).
242. *Id.* at 957 (Sotomayor, J., concurring).
243. Kerr, *Mosaic*, *supra* note 181, at 315.
244. *Id.*
245. *Id.* at 316.
246. *Id.* at 316-17.

A. DOCTRINAL FOUNDATION FOR QUALITATIVE LIMITS ON THIRD-PARTY DISCLOSURES

As discussed in depth above,[247] "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[248] Consequently, according to *Maryland v. Smith*, phone users can "claim no legitimate expectation of privacy" in the "numerical information [conveyed] to the telephone company."[249] This is because in dialing numbers on a telephone, and thus revealing that information to a third party, a telephone user "assume[s] the risk that the company w[ill] reveal to the police the *numbers* he dialed."[250] According to *United States v. Miller*, this is so even if the information revealed to a third party is "made available to [the third party] for a limited purpose."[251] Relying on *Katz v. United States*, the Court in *Miller* recognized "that a 'search and seizure' become[s] unreasonable when the Government's activities violate 'the privacy upon which [a person] justifiably relie[s]'"; however, the Court recognized that *Katz* "stressed that '[w]hat a person *knowingly exposes to the public* . . . is not a subject of Fourth Amendment protection.'"[252] As such, according to the third-party disclosure doctrine established in *Miller* and applied in *Smith*, disclosures are not limited by the purpose for which the information is disclosed, but rather disclosures are limited only by what information a person *knowingly exposes to the public*.

This view of third-party disclosures is consistent with the Court's general Fourth Amendment jurisprudence. For instance, in *Bond v. United States*,[253] the Supreme Court held that held that "a law enforcement officer's physical manipulation of a bus passenger's carry-on luggage violated the Fourth Amendment's proscription against unreasonable searches."[254] In doing so, the Court recognized that the defendant "expects," or assumes the risk, "that other passengers or bus employees may move [luggage] for one reason or another."[255] However, said the Court, the passenger "does not expect that other passengers or bus employees will, as a matter of course, feel the [luggage] in an exploratory manner."[256] Thus, by merely exposing an opaque travel bag to the

247. *See supra* Part I.
248. Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
249. *Id.* at 744.
250. *Id.* (emphasis added).
251. United States v. Miller, 425 U.S. 435, 442 (1976).
252. *Id.* (quoting *Katz v. United States*, 389 U.S. 347, 351, 353 (1967)) (alteration in original) (emphasis added).
253. Bond v. United States,529 U.S. 334 (2000).
254. *Id.* at 335.
255. *Id.* at 337.
256. *Id.* at 339.

world of bus passengers and bus employees, the defendant did not by that act knowingly expose his belongings to "physical manipulation" beyond ordinary handling.[257]

Similarly, the Court's "assumption of risk" line of cases, which provide the foundation for the Court's "third-party disclosure" doctrine, hold that what a person entrusts to a supposed confidant is "not protected by the Fourth Amendment when it turns out that the colleague is a government agent regularly communicating with the authorities."[258] This is so, because the Fourth Amendment does not "protect[] a wrongdoer's misplaced belief that a person to whom he *voluntarily confides* his wrongdoing will not reveal it."[259] However, this result pertains only to what a person *knowingly* exposes to the supposed confidant. Thus, in *Gouled v. United States*,[260] the Court held that a business associate of the defendant who gained entrance to the defendant's home by "pretending to make a friendly call upon the defendant" violated the Fourth Amendment when he "subsequently and secretly [searched defendant's papers] in his absence."[261]

The Court later elaborated on the significance of *Gouled* in *Lewis v. United States*.[262] There the Court stated that in *Gouled* there was "no difficulty concluding that the Fourth Amendment had been violated by the *secret* and general ransacking, notwithstanding" the fact that the defendant had voluntarily admitted the informant in to his home.[263] In *Lewis*, the Court ultimately held that an undercover purchase of marijuana by a government agent in the defendant's home did not violate the Fourth Amendment.[264] The Court distinguished the facts of *Gouled* by noting "the petitioner invited the undercover agent to his home for the *specific purpose* of executing a felonious sale of narcotics."[265] Thus, the defendant in *Lewis*, unlike the defendant in *Gouled*, knowingly exposed his criminal acts to his visitor. Further, noted the Court, the undercover agent did not "see, hear, or take anything that was not *contemplated*, and in fact *intended*, by petitioner as a necessary part of his illegal business."[266] Just as a private person may enter another's home

257. *Id.* at 338-39.
258. *E.g.*, United States v. White, 401 U.S. 745, 749 (1971).
259. Hoffa v. United States, 385 U.S. 293, 302 (1966) (emphasis added).
260. Gouled v. United States, 255 U.S. 298 (1921), *abrogated on other grounds by* Warden v. Hayden, 387 U.S. 294 (1967).
261. *Gouled*, 255 U.S. 298, *abrogated on other grounds by Warden*, 387 U.S. at 304, 306.
262. Lewis v. United States, 385 U.S. 206 (1966).
263. *Id.* at 210 (emphasis added).
264. *Id.* at 209-11.
265. *Id.* at 210 (emphasis added).
266. *Id.* (emphasis added).

for the purposes contemplated by the invitation, "[a] government agent . . . may accept an invitation to do business and may enter upon the premises for the very purposes *contemplated by the occupant*."[267] However, the scope of the invitation is limited by the subject matter contemplated by the occupant and, where an informant or government agent seeks information beyond what is contemplated, the Fourth Amendment is implicated. [268]

Concurring in *Florida v. Jardines*,[269] Justice Kagan employed similar reasoning in concluding that abuse of an implied license by government agents "invaded [the] 'defendant's reasonable expectation of privacy.'"[270] Although agreeing with Justice Scalia's treatment of the "case under a property rubric," Justice Kagan wrote "to note that [she] could just as happily have decided it by looking to [the defendant's] privacy interests."[271] Justice Kagan argued that police officers should be prevented from abusing an implied license to approach a home and knock on the door by "standing in an adjacent place and 'trawl[ing] for evidence with impunity,'" thus "insist[ing] on maintaining the 'practical value'" of the Fourth Amendment.[272] Although focusing, as did the Court in *Kyllo*, on the "'firm' and . . . 'bright' line at 'the entrance to the house,'"[273] Justice Kagan's concurrence should be read as indicating that the constitutional problem with the police conduct at issue in *Jardines* was that the officers "used a 'device . . . not in general public use' . . . to explore details of the home'" that those officers could not have discovered from a lawful vantage point—i.e., merely approaching the defendant's door and knocking.[274]

Although turning on a trespass analysis, Justice Scalia's majority opinion tracks with the analysis of Justice Kagan's concurrence. There, Justice Scalia explained that certain "invitation[s] . . . inhere in the very act of hanging a knocker."[275] Or, put differently, a person assumes certain risks by inviting others to knock on his door. Thus, "[t]o find a visitor knocking on the door is routine (even if sometimes unwelcome);

---

267. *Id.* at 211 (emphasis added).

268. *See Lewis*, 385 U.S. at 211 ("Of course, this does not mean that, whenever entry is obtained by invitation and the locus is characterized as a place of business, an agent is authorized to conduct a general search for incriminating materials; a citation to the *Gouled* case is sufficient to dispose of that contention." (citation omitted)).

269. For a discussion on *Florida v. Jardines*, see *supra* Part IV.B.

270. *See* Florida v. Jardines, 133 S. Ct. 1409, 1418 (2013) (Kagan, J., concurring) (quoting Katz v. United States, 389 U.S. 347, 360 (1967)).

271. *Id.* (Kagan, J., concurring).

272. *Id.* (Kagan, J., concurring) (first alteration in original) (quoting Florida v. Jardines, 133 S. Ct.1409, 1414 (2013) (majority opinion)).

273. *Id.* at 1419. Florida v. Jardines, 133 S. Ct. 1409, 1419 (2013) (Kagan, J., concurring) (quoting Kyllo v. United States, 533 U.S. 27, 40 (2001)).

274. *See id.* at 1418 (Kagan, J., concurring).

275. *Id.* at 1416.

to spot that same visitor exploring the front path with a metal detector . . . before saying hello and asking permission, would inspire most of us to—well, call the police."[276] Indeed, just as the assumption of risk under the Fourth Amendment is limited by the extent to which a person reveals information to third parties, "[t]he scope of a license—express or implied—is limited not only to a particular area but also to a specific purpose."[277] Formed as an assumption of risk analysis, where "the background social norms that invite a visitor to the front door" to knock, it can be said that the occupant of the home assumes the risk that police officers at the door will observe possible criminal activity with the unaided ear or eye.[278] However, those same social norms do not allow officers "to conduct a search."[279]

At bottom, under the line of cases discussed above, although it is well established that people lack a reasonable expectation of privacy in information knowingly disclosed to third parties, the assumption of risk doctrine, and the included third-party disclosure doctrine, are not without limits. Indeed, the principle drawn from the above cases is that a defendant assumes the risk of unauthorized disclosure only as to those activities and information that a defendant *knowingly* entrusts to a third party. Where an informant or undercover government agent discovers information by searching beyond what the defendant *knowingly* exposed to the third party, the Fourth Amendment is implicated. The need to remember the rationale of the third-party disclosure doctrine is of paramount importance in the digital age because, as the Court noted most recently in *Riley v. California*,[280] courts must determine whether the application of a doctrine to a given set of circumstances "would 'untether the rule from the justifications underlying . . . '" the third-party disclosure doctrine.[281]

B. A QUALITATIVE TEST TO GAUGE THE CONSTITUTIONALITY OF THE NSA BULK TELEPHONY METADATA COLLECTION PROGRAM

In applying a qualitative test to Fourth Amendment issues arising out of the NSA's bulk telephony metadata collection program, courts

---

276. *Jardines*, 133 S. Ct. at 1416.

277. *See Id*.

278. *See, e.g.*, Kentucky v. King, 131 S. Ct. 1849, 1862-63 (2011) (upholding a search supported by exigent circumstances where officers knocked on defendant's door, announcing their presence, and heard what they believed was the destruction of evidence from within defendant's apartment).

279. *Jardines*, 133 S. Ct. at 1416.

280. Riley v. California, 134 S. Ct. 2473 (2014).

281. *Id.* at 2485 (quoting Arizona v. Gant, 556 U.S. 332, 343 (2009)).

should ask two questions. First, what do telephone users reasonably expect, *ex ante*, to reveal when they disclose numbers dialed to telephone companies. Second, courts should ask if the NSA's bulk telephony mass collection program is capable of exposing information beyond what telephone users expect to reveal when disclosing numbers dialed to telephone companies. If it is, then courts should rule that the NSA's metadata collection program implicates the Fourth Amendment.

As far as what telephone users reasonably expect *ex ante* when disclosing numbers dialed to third-party telephone companies, it is clear that people do not "entertain any actual expectation of privacy in the numbers they dial."[282] Thus, no matter the technology used, if it discloses only the numbers a person dials, there can be no Fourth Amendment violation. This is because "all subscribers realize that they must 'convey' phone numbers to the telephone company" not only to complete the call, but also so "that the phone company . . . [can] mak[e] permanent records of the numbers they dial."[283] Similarly, because data obviously collected by telephone companies includes "incoming . . . phone numbers, call duration, text and data usage,"[284] which is "no more than pen register . . . data," courts have concluded that telephone users cannot claim a reasonable expectation of privacy in "'call origination, length, and time of call.'"[285] Thus, no matter the technology employed, if it discloses only the numbers a particular person dials, where those calls originated, how long those calls lasted, and what numbers contacted a person directly, there can be no Fourth Amendment violation.

However, what is less clear is whether telephone users reasonably expect that the information they disclose to telephone companies will be compiled with others' similarly disclosed information in a manner capable of creating a rich mosaic of social connection, including people who a particular person might never have been in direct contact with.[286] Indeed, such a rich mosaic goes beyond the first-level of connections that one reasonably could expect to reveal in their dealings with a third-party telephone company and potentially exposes "a wealth of detail about her familial, political, professional, religious, and sexual associations."[287] To be sure, such great detail is materially different from the

---

282. Smith v. Maryland, 442 U.S. 735, 742 (1979).

283. *Id.*

284. *See* Zachary Ross, Note, *Bridging the Cellular Divide: A Search for Consensus Regarding Law Enforcement Access to Historical Cell Data*, 35 CARDOZO L. REV. 1185, 1191 (2014).

285. *E.g.*, United States v. Reed, 575 F.3d 900, 914 (9th Cir. 2009).

286. *See supra* Part II (discussing the scope of the NSA's bulk telephony metadata collection program).

287. *Cf.* United States v. Jones, 132, S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (expressing concern that pervasive GPS monitoring goes beyond what more limited surveillance could obtain by "generat[ing] a precise, comprehensive record of a person's

information that a "one-time, targeted request for data regarding an individual suspect in a criminal investigation" would produce.[288] Indeed, a particular telephone customer might not even be aware of what such a program would reveal about her. It is quite conceivable that an individual unwittingly has been in contact with a seemingly innocent associate who is actually involved in, or similarly unwittingly connected to individuals suspected of, terrorist activity. Such a very real possibility shows that aggregation of phone records will reveal information beyond what could be obtained from an individual's phone records alone. Accordingly, under the "assumption of risk" cases, it is difficult to say that simply by using a telephone a particular user invited law enforcement officers to aggregate that data with other similarly acquired data in order to discover further information regarding associations.[289] One might say, as Chief Justice John Roberts did in *Riley v. California* regarding searches of cell phone data incident to arrest, that to argue the information available through the NSA's bulk telephony metadata collection program is indistinguishable from the information revealed through the use of a pen register in *Smith* "is like saying a ride on horseback is materially indistinguishable from a flight to the moon."[290]

---

public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations").

288. *See* Klayman v. Obama, No. 1:13-CV-0881, 2013 WL 6598728, at *19 (D.D.C. Dec. 16, 2013).

289. *Cf.* Florida v. Jardines, 133 S. Ct. 1409, 1416 (2013) ("An invitation to engage in canine forensic investigation assuredly does not inhere in the very act of hanging a knocker.").

Justice Scalia's dissent in *Maryland v. King*, too, is illustrative on this point. His dissent distinguished the intrusion of an arrestee's privacy that certain noninvestigative searches occasion, from investigative searches for evidence of crime "when there is no basis for believing the [arrestee] is guilty of the crime or in possession of incriminating evidence." *See generally* Maryland v. King, 133 S. Ct. 1958, 1980-90 (2013) (Scalia, J., dissenting). The majority in *Maryland v. King* reasoned that because "[t]he expectations of privacy of an individual taken into police custody 'necessarily [are] of a diminished scope," *Id.* at 1978 (alteration in original) (quoting Bell v. Wolfish, 441 U.S. 520, 557 (1979)), and because the buccal swab at issue occasioned only "[a] brief intrusion of an arrestee's person," *Id.* at 1979, the search at issue was "reasonable under the Fourth Amendment." *Id.* at 1980. Justice Scalia, on the other hand, urged that the type of intrusion that accompany suspicionless searches for the purposes of identification were materially different from the intrusion at issue, which involved the taking of DNA samples to be "checked against the Unsolved Crimes Collection," palpably investigative in nature *See Id.* at 1985-86 (Scalia, J., dissenting).

Put differently for purposes of analysis, Justice Scalia's dissent in *Maryland v. King* can be read as arguing that while an arrestee may expect to be subject to certain, noninvestigative searches upon arrest, it does not follow that the arrestee's acknowledged diminished expectation of privacy, clears the path for even minimally invasive investigative searches aimed at securing possible evidence of yet-to-be-discovered crimes.

290. Riley v. California, 134 S. Ct. 2473, 2488 (2014).

As such, this Article argues that, although individuals cannot claim a reasonable expectation of privacy in the numbers they dial or the numbers that contact them ("first-level contacts"), it cannot be said that they, by the simple act of using a phone, assume the risk of exposing a broad mosaic of social connections that reaches telephone users with whom they have never been in direct contact with.

As to first-level contacts, "[t]he essence of the theory is that by allowing information or records respecting yourself to come into the possession of another private party, you waive privacy rights" and the government is free to discover those contacts.[291] However, the information discoverable through an aggregation of all telephone users' first-level contact data "differ[s] for a number of reasons."[292] First, any particular user does not knowingly reveal anything regarding his or her associations beyond the first-level of contacts. "Moreover, the information in the form collected is not known by him to exist anywhere nor does he consent to its compilation."[293] Indeed, there is not necessarily a reason for any individual telephone customer to know, or even suspect, that the details a particular first-level contact discloses to a third-party telephone company will then be compiled and used to discover information beyond what she knowingly disclosed.[294] Even in the digital age, where massive amounts of information are necessarily disclosed to third parties on a daily basis, society recognizes the right of individuals to control what third-parties disclose about them without their prior consent. For instance, Google allows users to limit what information is collected and used by third parties, thus empowering users to control the extent of their own exposure to third-parties.[295]

Accordingly, when assessing the NSA's bulk telephony metadata collection program, courts should first find that telephone users entertain a reasonable expectation of privacy in any connections they might have beyond first-level contacts. Indeed, if they do have connections beyond that level, they have manifested a subjective expectation of privacy in those connections by not contacting them directly by phone. Free-

---

291. *See* United States v. Choate, 576 F.2d 165, 205 (9th Cir. 1978) (Hufstedler, J., concurring and dissenting).

292. *Id.* (Hufstedler, J., concurring and dissenting).

293. *Id.* (Hufstedler, J., concurring and dissenting).

294. *See cf. id.* (9th Cir. 1978) (Hufstedler, J., concurring and dissenting) ("There is no reason for a mail cover suspect to assume that a list of all his correspondents has been compiled.").

295. *See, e.g.*, Jack Schofield, *Google's Privacy Settings—Controlling Your Information*, GUARDIAN (Mar. 1, 2012, 3:59 PM), http://www.theguardian.com/technology/2012/mar/01/google-privacy-settings-controlling-information.

dom of association is an essential aspect of a democratic society and, [296] for whatever reason, people might not want third parties or the government to know the extent of their associations. As Professors Gray and Citron argue, technologies that subvert such manifested expectations of privacy regarding associations threaten "liberty and democratic culture."[297] Thus, given the ever-increasing importance of technology in the digital age,[298] courts also should recognize that maintaining privacy in associations beyond those first-level conducts is an expectation of privacy that society is prepared to recognize in the digital age.[299] As evidence of this societal recognition of an individual's right to control the scope of personal information disclosed to third parties in the digital age, one need look no further than the various "how to" guides on controlling Internet privacy and the appeal of services marketing enhanced privacy protection.[300] Indeed, enhanced privacy features have become a selling point for consumers of high-technology products and services. By way of example, in a recent consumer protection oriented "marketing pitch," both Apple and Google have "move[d] . . . to put some smartphone data out of reach of police and the courts."[301]

Courts should then turn to the technology used in a given surveillance program. The question becomes whether the technology at issue reveals more about a particular individual than could be garnered using only the first-level contact data disclosed to telephone companies. As applied to the NSA program, courts should ask whether the NSA bulk

---

296. Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 783 (2008).

297. Gray & Citron, *Quantitative Privacy*, *supra* note 175, at 82 (discussing the "dangers of powerful data aggregation and analysis technologies"); *see also* Jack M. Balkin, Essay, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 12 (2008) ("[M]odern societies ha[ve] become increasingly focused on watching and measuring people in order to control them . . . . Government's most important technique of control is no longer watching or threatening to watch. It is analyzing and drawing connections between data . . . . [D]ata mining technologies allow the state . . . to record perfectly innocent behavior that no one is particularly ashamed of and draw surprisingly powerful inferences about people's behavior, beliefs, and attitudes.").

298. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("[In] the digital age . . . people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks").

299. *See* Klayman v. Obama, No. 1:13-CV-0881, 2013 WL 6598728, at *19 (D.D.C. Dec. 16, 2013).

300. *E.g.*, Melanie Pinola, *A Guide to Google+ Privacy and Information Control*, LIFEHACKER (Aug. 8, 2011, 8:00 AM), http://lifehacker.com/5827683/a-guide-to-google%252B-privacy-and-information-control ("[O]ne of the main reasons so many people are interested in [Google+] over Facebook is Google+'s proclaimed focus on protecting users' privacy.").

301. *See* Devlin Barrett & Danny Yadron, *New Phone Protections Alarm Law Enforcement*, WALL ST. J., Sept. 23, 2014, at A1.

telephony metadata collection goes beyond what would be discoverable from examination of an individual's first-level contacts, thereby infringing on particular telephone user's reasonable expectations of privacy. The focus on technology here is important, because there is no question as to whether law enforcement officials could manually collect all of the information disclosed to third-party telephone companies and manually query it looking for connections to known terrorist numbers. The concern here is that the use of technology-enhanced aggregation techniques will decrease the cost of such extensive surveillance so as to allow law enforcement access to information to that which they could not have otherwise feasibly attained.[302]

Framed in this manner, the answer to the question applied to the NSA telephony metadata collection program is straightforward. By its very terms, the NSA program collects and aggregates telephony metadata because the aggregation reveals more information than could be gleaned from looking at individual, first-level contacts in isolation.[303] Indeed, the program "is not feasible unless NSA analysts have access to telephony metadata in bulk, because they cannot know which of the many phone numbers might be connected until the conduct analysis" of the aggregate database.[304] As the Government admits, limiting analysis to the first-level contacts of particular telephone users "would impede the ability to *identify a chain of contacts* between telephone numbers."[305]

Accordingly, if courts recognize a reasonable right to privacy in associations beyond first-level contacts, it is evident that the bulk telephony metadata collection program is capable of discovering information regarding a particular telephone user beyond that which the user *knowingly* exposed to a third-party. To be sure, that is the very purpose of the bulk telephony metadata collection program. As such, the program cannot be justified under the third-party disclosure doctrine, which is limited in scope to information that individuals knowingly disclose to a third-party—i.e., first-level contacts. Thus, courts should find that the NSA bulk telephony metadata collection program implicates the Fourth

---

302. *See* Gray & Citron, *Quantitative Privacy*, *supra* note 175, at 102 (expressing concern regarding police surveillance technology that "is capable of broad and indiscriminate . . . by its nature, *or* is sufficiently *inexpensive* and *scalable* so as to present *no practical barrier* against its broad and indiscriminate use") (emphasis added)); *see also Jones*, 132 S. Ct. at 963 (Alito, J., concurring) ("Traditional surveillance for any extended period of time was *difficult* and *costly* and therefore rarely undertaken. (emphasis added)).

303. ADMIN. TELEPHONY METADATA WHITE PAPER, *supra* note 75, at 13 ("NSA employs a multi-tiered process of analyzing the data in an effort to identify *otherwise unknown* connections between telephone numbers associated with known or suspected terrorists and to other telephone numbers." (emphasis added)).

304. *Id.*

305. *Id.* (emphasis added).

Amendment.

It may well be that statutory rather than judicial regulation of programs like the NSA's bulk telephony metadata collection program is proper. However, as Justice Alito has explained, so long as the legislature fails to act to constrain such practices to comport with the Fourth Amendment, "the best that [the Court] can do . . . is to apply existing Fourth Amendment doctrine and ask whether the use of [technologically-enhanced surveillance] in a particular case involve[s] a degree of intrusion that a reasonable person would not have anticipated."[306] This Article argues that, when viewed in light of the Fourth Amendment rubric set forth above, the NSA bulk telephony metadata collection program occasions an intrusion that offends society's reasonable expectations of privacy. Thus, despite the fact that the NSA's metadata collection program purportedly comports with the requirements of Section 215 of the PATRIOT Act and is conducted in pursuit of legitimate law enforcement ends, courts "cannot forgive the requirements of the Fourth Amendment in the name of law enforcement."[307]

This is not to say that such a program, or a program similar to it, is "barred under the [Fourth] Amendment."[308] Rather, such a program will comport with the Fourth Amendment only when it is regulated in such a manner as to prevent invasions "contrary to the command of the Fourth Amendment."[309] As discussed above, the NSA bulk telephony metadata collection is not so regulated. Indeed, the broad scope and indefinite duration of the program "permits a[n] . . . invasion . . . by general warrant, contrary to the command of the Fourth Amendment."[310]As such, in the absence of further statutory regulation, it is for the courts to ensure that law enforcement officials adhere to the commands of the Fourth Amendment and allow continuation of the NSA bulk telephony metadata collection program only if the Government can prove that special needs justify exemption from the warrant requirement.[311]

---

306. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

307. *See* Berger v. New York, 388 U.S. 41, 62 (1967).

308. *See id.* at 63.

309. *See id.*

310. *See id.*; *see also* Klayman v. Obama, No. 1:13-CV-0881, 2013 WL 6598728, at *20 (D.D.C. Dec. 16, 2013) (characterizing the NSA bulk telephony metadata collection program as "almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States").

311. *See, e.g.*, Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 674 (1989) (allowing warrantless drug searches "[i]n light of the extraordinary safety and national security hazards that would attend the promotion of drug users to positions that require the carrying of firearms or the interdiction of controlled substances").

CONCLUSION

In light of the revelations regarding the astounding amount of information the NSA has been aggregating from the telephone networks of United States citizens, it is indeed time that the Court reexamines the continued vitality of its third-party disclosure doctrine in the digital age. The idea that an individual can claim no reasonable expectation of privacy in information voluntarily disclosed to third parties should depend on an individual's knowing, voluntary assumption of the risk that the third party will not keep the information disclosed a secret. However, the Fourth Amendment holds that information not disclosed to those third parties should remain undiscoverable absent a warrant or some other exception or excusal from the warrant requirement of the Fourth Amendment. Where the NSA aggregates bulk amounts of telephony metadata, it is able to discover information about any particular individual that goes beyond what any one of those individuals knowingly disclosed to a third party. Such discoveries reach past information voluntarily disclosed to third parties to uncover information that would not otherwise have been ascertainable absent the use of enhanced technology. It simply cannot be that individuals forfeit reasonable expectations of privacy in information that they themselves did not disclose to third parties on the basis of an unknown disclosure of that information to a third party by another individual.[312] Thus, courts should recognize a reasonable expectation of privacy in an individual's associations beyond first-level contacts and should conclude that the NSA's bulk telephony metadata collection program infringes on that expectation of privacy by aggregating data in order to discover information not otherwise discoverable from any one particular set of first-level contacts.

312. *See, e.g.*, United States v. Choate, 576 F.2d 165, 205 (9th Cir. 1978) (Hufstedler, J., concurring and dissenting) (questioning whether a recipient of mail forfeits expectations of privacy when the sender choses to convey information to him by mail, because "the recipient of mail does not knowingly reveal anything").