THE END OF Smith v. Maryland?: The NSA’s Bulk Telephony Metadata Program and the Fourth Amendment in the Cyber Age

Alexander Galicki*

INTRODUCTION

In June 2013, The Guardian newspaper disclosed that the United States National Security Agency (“NSA”) has been collecting the telephony metadata for virtually all telephone calls made inside the United States for the last seven years.1 The existence of the NSA program was disclosed to Guardian reporter Glenn Greenwald by Edward Snowden, a former systems operator for NSA contractor Booz Allen Hamilton.2 This Note will argue that the NSA’s bulk collection of telephony metadata constitutes a “search” within the meaning of the Fourth Amendment to the U.S. Constitution. If the NSA’s bulk collection of metadata does indeed constitute a “search,” the NSA program is presumptively unconstitutional as it is carried out on a warrantless and suspicionless basis. The Fourth Amendment states, in full:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.3

As any law student learns in introductory criminal procedure, the Fourth Amendment speaks only of “unreasonable searches and seizures.”4 For that reason, the initial inquiry in any Fourth Amendment analysis is always whether a “search” has even taken place. Under the Supreme Court’s “search” jurisprudence, if a particular type of governmental intrusion constitutes a “search,” the substan-

* Georgetown University Law Center, J.D. expected 2015; University of Southern California, B.A., International Relations 2010 © 2014, Alexander Galicki. Special thanks to Professors Don Wallace, Laura Donohue, James Zirkle, Kenneth Lazarus, Paul Butler, C. Dean McGrath, and Martin Lederman. I would also like to thank Professor Paul Butler for first sparking my interest in the Fourth Amendment.


3. U.S. CONST. amend. IV.

4. Id. (emphasis added).
tive requirements of the Fourth Amendment apply and the government must generally have obtained a warrant issued upon probable cause. By contrast, if there has been “no ‘search’ at all,” the government can constitutionally engage in the type of conduct at issue without a warrant or any level of suspicion. Defining when a “search” has taken place, therefore, is crucial because in many cases it draws the line between when the government may engage in potentially warrantless and suspicionless intrusions into the private sphere and when it must first appear before a neutral and detached magistrate to obtain a warrant issued upon probable cause. Accordingly, the Court has had to strike the appropriate balance between individual liberty and law enforcement through its “search” jurisprudence. On the one hand, the Fourth Amendment serves as an important check on governmental power and the Founding Fathers included the provision after having dealt with the British Crown’s practice of using “general warrants” in the American colonies. On the other hand, the Fourth Amendment inherently stifles effective law enforcement, an essential function of any sovereign state.

Seeking to balance these countervailing interests, the Court established the modern test for determining whether a “search” has occurred in United States v. Katz. Justice Harlan, in his now famous concurrence, stated that a “search” has taken place when an individual has an actual (subjective) expectation of privacy in the place to be searched, and that expectation is one which society would accept as reasonable. Ten years later, in Smith v. Maryland, the Court held that a single criminal defendant did not retain a reasonable expectation of privacy in twenty-four hours of telephone dialing information, which he voluntarily transmitted to the telephone company to complete his calls. However, Smith stands as merely one example of the Court’s broader view that under the Katz test an individual does not retain a legitimate expectation of privacy in information that he or she voluntarily exposes to a third party or the public at-large (commonly known as the “third-party doctrine”). As the Supreme Court has explained:

>[The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. In other words, a person cannot have a reasonable expectation of

---

5. Kyllo v. United States, 533 U.S. 27, 32 (2001) (“But in fact we have held that visual observation is no ‘search’ at all—perhaps in order to preserve somewhat more intact our doctrine that warrantless searches are presumptively unconstitutional.”).
8. Id. at 361 (Harlan, J., concurring).
privacy in information disclosed to a third party. The Fourth Amendment simply does not apply.\textsuperscript{10}

Supporters of the constitutionality of the NSA program, including the Obama Administration, point to the third-party doctrine and especially \textit{Smith v. Maryland} as a simple answer to the NSA program.\textsuperscript{11} They contend that when the government collects the telephony metadata for all phone calls made inside the United States there simply is no “search” because, as in \textit{Smith v. Maryland}, customers have voluntarily turned over their dialing information to the telephone company.\textsuperscript{12}

While it is true that the Court has a long line of precedent supporting the third-party doctrine, even before the Snowden disclosures, the Court had begun to chip away at the doctrine.

The cyber age challenges the third-party doctrine in two significant ways. First, American citizens voluntarily expose much more information to third parties and to the public at-large: Facebook, cellphones, web browsing history, and metadata to name a few. Second, that exposed information can now be analyzed using new technologies to reveal intimate details that were previously undetectable: logarithms, thermal guns, and complex databases that permit the storage and retrieval of information dating back five years. In light of these recent technological advances, the Court has been struggling with whether to abandon the third-party doctrine wholly or in part. It came close to addressing the question in \textit{United States v. Jones},\textsuperscript{13} but instead wrote a narrow opinion by relying on trespass analysis.\textsuperscript{14}

The NSA program is now on appeal at the Court of Appeals for the Second and D.C. Circuits,\textsuperscript{15} and the Supreme Court will likely be presented with a powerful opportunity to rearticulate a modern conception of the third-party doctrine.

\textsuperscript{10} Orin S. Kerr, \textit{The Case for the Third-Party Doctrine}, 107 MICH. L. REV. 561, 563 (2009) (quoting United States v. Miller, 425 U.S. 435, 443 (1976)); see \textit{Katz}, 389 U.S. at 361 (Harlan, J., concurring) ("[O]bjects, activities, or statements that he exposes to the ‘plain view’ of outsiders are not ‘protected’ because no intention to keep them to himself has been exhibited.").

\textsuperscript{11} A\textsc{dministration White Paper, Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act 20 (2013) [hereinafter “OBAMA WHITE PAPER”].

\textsuperscript{12} Id.

\textsuperscript{13} 132 S. Ct. 945 (2012). In \textit{Jones}, the Court addressed whether the government had engaged in a Fourth Amendment “search” when it installed a GPS device on the defendant’s vehicle and tracked his public movements over the course of one month. \textit{Id.} at 948. While the Court was plainly confronted with the question of whether \textit{Smith} remained good law in cases where the government uses sophisticated technology to collect large amounts of information voluntarily exposed to the public, the majority opinion chose to rely on a physical “trespass” conception of the Fourth Amendment to rule that the government had conducted a “search.” \textit{Id.} at 949. However, a plurality of the Justices embraced the idea that even under \textit{Katz}, the month-long monitoring constituted a “search.” \textit{Id.} at 954–57 (Sotomayor, J., concurring); \textit{Id.} at 962 (Alito, J., concurring).

\textsuperscript{14} \textit{Id.} at 949.

This Note will argue that the Court should follow its recent trend in cases like *Jones* and rule that the NSA’s bulk collection of telephony metadata constitutes a “search” under the Fourth Amendment. Section I will provide a historical overview of the Court’s third-party doctrine jurisprudence. Section II will examine more recent cases indicating that the Court might be retreating from its decision in *Smith v. Maryland*. Section III will then give factual background on the NSA’s bulk telephony metadata program and analyze two recent decisions, *Klayman v. Obama* and *ACLU v. Clapper*, which issued contrary rulings on the constitutionality of the NSA program and are now on appeal at the Second Circuit and the D.C. Circuit. Finally, in Section IV, I will conclude that if the Supreme Court is asked to review the constitutionality of the NSA program, it should hold that the long-term bulk collection of telephony metadata constitutes a “search” for which a warrant based on probable cause is required under the Fourth Amendment.

I. THE SUPREME COURT’S THIRD-PARTY DOCTRINE

This Section will examine the Supreme Court’s “third-party doctrine.” Part A will explore the historical origins of the doctrine, which, according to Professor Orin Kerr, can be traced to several early Supreme Court cases involving the government’s use of secret agents. Part B will then analyze the Court’s preservation of the third-party doctrine following its decision in *Katz v. United States* and look at the expansion of the doctrine in a series of cases involving business records. Finally, Part C will examine a separate line of cases, establishing that, as with information disclosed to a third-party, an individual does not retain a reasonable expectation of privacy in information exposed to the public at-large.

A. The Historical Origins of the Third-Party Doctrine

According to Professor Orin Kerr, the Supreme Court first addressed the question of whether evidence obtained by secret agents could be used as evidence in a criminal proceeding in *On Lee v. United States*. In that case, Lee was charged with selling and conspiring to sell one pound of opium in violation of federal law. While out on bail and prior to trial, Lee was working at his laundry when an old friend, Chin Poy, engaged him in conversation during the course of which Lee made incriminating statements. However, it turned out that Poy was actually an undercover agent for the Government wearing a small microphone “wire,” and the

---

20. Kerr, supra note 10, at 569–70.
21. 343 U.S. 747 (1952); Kerr, supra note 10, at 566–68.
23. *Id.* at 749.
statements were later used against Lee in court.24 Lee asserted that the government had violated the Fourth Amendment because Poy wearing a wire was comparable to installing a listening device or bug inside of Lee’s laundry.25 The Court rejected Lee’s argument, upholding the government’s use of Poy’s recording at trial.26 Justice Jackson explained that Lee “was talking confidentially and indiscreetly with one he trusted.”27 And it did not matter that Poy was wearing a wire because the recording was “with the connivance of one of the parties” to the conversation.28

The Court then expanded on this line of precedent in three cases decided during the 1960s.29 In Lopez v. United States, the defendant attempted to bribe an IRS agent who was wearing a concealed wire.30 The recorded statements and the agent’s testimony were admitted as evidence against him at trial.31 The Court rejected the defendant’s argument that the recording of the conversation had been obtained in violation of his rights under the Fourth Amendment.32 Next, in Lewis v. United States, the defendant invited an undercover federal narcotics agent into his home on two occasions and sold him large quantities of marijuana.33 The narcotics agent subsequently testified at trial about what he had seen and heard in his encounter with the defendant.34 Justice Warren, rejecting any claim under the Fourth Amendment, explained that “[d]uring neither of his visits to [the defendant’s] home did the agent see, hear, or take anything that was not contemplated, and in fact intended, by [the defendant] as a necessary part of his illegal business.”35 In other words, as in On Lee and Lopez, the defendant was “talking confidentially and indiscreetly with one he trusted,”36 who was “there with [the defendant’s] assent.”37 As a result, the defendant had assumed the risk that the undercover agent might disclose what he had seen and heard to other parties. The Court also expressed a broader public policy concern: if the deceptions by the agent were barred in this instance, “we would come near to a rule that the use of undercover agents in any manner is virtually unconstitutional per se.”38

24. Id. at 749–50.
25. Id. at 751–54.
26. Id. at 751.
28. Id. (quoting On Lee, 343 U.S. at 754).
29. Id. at 567–568 (explaining that the Court reached the same result a decade later in Lopez, Lewis, and Hoffa).
31. Id. at 432.
32. Id. at 437–39.
34. Id. at 208; see also Kerr, supra note 10, at 568.
35. Lewis, 385 U.S. at 210.
37. Lopez, 373 U.S. at 439.
Finally, the Court reached the same result in *Hoffa v. United States*, in which the famous leader of the Teamsters union, Jimmy Hoffa, had made incriminating statements to his colleague Edward Partin about his attempts to bribe members of the jury in the Test Fleet trial. It turned out that Partin was working for the government, and Hoffa was subsequently convicted, with the government relying largely on Partin's testimony at trial. Directly citing *Lopez* and *On Lee*, the Court held that the government's use of Partin's testimony did not violate the Fourth Amendment. The Court explained that Partin "was in the suite by invitation, and every conversation which he heard was either directed to him or knowingly carried on in his presence. . . . [Hoffa] was relying upon his misplaced confidence that Partin would not reveal his wrongdoing." Ultimately, the Court concluded that 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.

**B. The Third-Party Doctrine After Katz**

As the 1960s came to a close, the Supreme Court's third-party doctrine was firmly established, beginning with *On Lee* in 1952 and ending with *Hoffa* in 1966. However, the doctrine was analytically rooted in the Court's broader theoretical conception of what constitutes a "search" under the Fourth Amendment, established by the Court's decision in *Olmstead v. United States*. Subpart 1 will explain the Court's holding in *Olmstead* and Subpart 2 will then analyze whether *Katz v. United States*, which overruled *Olmstead*, abrogated the secret agents line of third-party doctrine jurisprudence. Subpart 3 will examine the Supreme Court's expansion of the third-party doctrine from secret agents to business records in a series of cases between 1973 and 1980. Finally, Subpart 4 will examine the Court's decision in *Smith v. Maryland*, which expanded the third-party doctrine to numerical telephone information voluntarily conveyed by customers to the telephone company and captured by a "pen register" installed by the government.
1. Olmstead v. United States: A Trespass Conception of the Fourth Amendment

Olmstead addressed the question of whether use of evidence of private conversations between defendants, intercepted through wire-tapping, amounted to an unconstitutional Fourth Amendment “search.”\(^{49}\) In that case, the defendants were convicted of conspiracy to import, possess, and sell liquor in violation of the National Prohibition Act.\(^{50}\) Four federal prohibition officers discovered the conspiracy largely through intercepting messages on the telephones of the conspirators over several months.\(^{51}\) Specifically, wires were “inserted along the ordinary telephone wires from the residences of four of the petitioners and those leading from the chief office. The insertions were made without trespass upon any property of the defendants.”\(^{52}\)

The Court held unequivocally that this did not constitute a “search” within the meaning of the Fourth Amendment, establishing the rule that governmental conduct only constitutes a “search” if it physically penetrates a constitutionally protected area.\(^{53}\) Justice Taft, writing for the majority, explained:

> The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. . . . Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house “or curtilage” for the purpose of making a seizure.\(^{54}\)

Thus, the Court’s ruling in Olmstead was firmly rooted in a concept of physical space, which served as a predictable barometer for detecting Fourth Amendment violations. Physically intruding into a home? That’s a search. Observing someone’s movements in an open field? That’s not a search. And the third-party doctrine made analytical sense under this framework, as conversations or verbal exchanges are not really physical spaces. Thus, so long as a governmental official was legally present in the space where he or she overheard or recorded a conversation (whether at home, or on the street), there was deemed to be no violation of the Fourth Amendment. In fact, in each of the Court’s third-party doctrine cases, discussed in the previous section, the undercover agent was legally present with the voluntary

---

49. *Olmstead*, 277 U.S. at 455.
50. *Id.*
51. *Id.* at 456–57.
52. *Id.* at 457.
53. *Id.* at 464, 466.
54. *Id.* at 466. *But see id.* at 478–79 (Brandeis, J., dissenting) (arguing that the wire-tapping was an unconstitutional intrusion into defendants’ privacy and that it was immaterial where the phones were tapped).
assent of the defendant under indictment, and for that reason, the defendant had effectively assumed the risk.

However, as the four dissenting opinions filed in *Olmstead* demonstrate, not everyone was content with this quasi-bright line rule. And it is also doubtful that the *Olmstead* majority truly appreciated the potential for advances in electronic surveillance or the extent to which law enforcement officials would come to rely on it as a means to investigate crime. However, the Court faithfully applied *Olmstead* for the next forty years until it opted to revisit the question of whether the Fourth Amendment protects citizens against anything other than physical governmental intrusions in *Katz v. United States*. In *Katz*, the Supreme Court finally overruled *Olmstead*, famously noting that “the Fourth Amendment protects people, not places.” The next section will explain the *Katz* decision and analyze how, if at all, it impacted the third-party doctrine.

2. The *Katz* Test and Secret Agents Revisited

It was a day reminiscent of a retro 1960s TV cop show. The setting was Los Angeles, and the suspect, Charles Katz, was making his way along the sidewalk, trailed by two FBI agents. Katz entered a public telephone booth and closed the door. The FBI agents, eager to listen in, attached a listening and recording device to the exterior of the booth. Unfortunately for Katz, they captured him transmitting bets or wagers to Miami and Boston. Katz was charged under an eight-count

55. See id. at 469–71 (Holmes, J., dissenting); id. at 471–85 (Brandeis, J., dissenting); id. at 485–88 (Butler, J., dissenting); id. at 488 (Stone, J., dissenting).

56. See, e.g., Goldman v. United States, 316 U.S. 129, 135 (1942) (refusing to overrule *Olmstead v. United States*). Writing for the majority in *Goldman*, Justice Roberts explained:

> The suggested ground of distinction is that the Olmstead case dealt with the tapping of telephone wires, and the court adverted to the fact that, in using a telephone, the speaker projects his voice beyond the confines of his home or office and, therefore, assumes the risk that his message may be intercepted. It is urged that where, as in the present case, one talks in his own office, and intends his conversation to be confined within the four walls of the room, he does not intend his voice shall go beyond those walls and it is not to be assumed he takes the risk of someone’s use of a delicate detector in the next room. We think, however, the distinction is too nice for practical application of the Constitutional guarantee and no reasonable or logical distinction can be drawn between what federal agents did in the present case and state officers did in the Olmstead case. The petitioners ask us, if we are unable to distinguish Olmstead v. United States, to overrule it. This we are unwilling to do.

Id.


58. Id. at 351.

59. Kerr, *supra* note 10, at 568 (explaining that the third-party doctrine survived the analytical switch to the *Katz* test).

60. *Katz*, 389 U.S. at 348–49.

61. Id. at 348, 352.

62. Id. at 348.

63. Id.
indictment for violating a federal statute. At trial, the government was permitted, over the defendant’s objections, to introduce the telephone conversations recorded by the FBI. After the Ninth Circuit affirmed Katz’s conviction, the Supreme Court granted certiorari, tasked with addressing whether the government had violated the Fourth Amendment. The case was Katz v. United States, and the Supreme Court would make Fourth Amendment history in establishing the Katz test, which is the modern method for determining whether the government has engaged in a “search” within the meaning of the Fourth Amendment.

The Supreme Court held that the government’s conduct in electronically eavesdropping on and recording the defendant’s words spoken into a telephone in an enclosed telephone booth constituted a “search” under the Fourth Amendment, even though the device used to carry out the surveillance did not physically penetrate the wall of the booth. As a result, the government’s failure to obtain a warrant prior to the surveillance violated the Fourth Amendment. Overturning Olmstead v. United States, Justice Harlan’s now-famous concurrence established a two-pronged test for determining whether a “search” has occurred: a person must have exhibited an actual (subjective) expectation of privacy in the place to be searched, and that expectation must be one which society is prepared to accept as reasonable.

But for our purposes, an important question remained unanswered: would the third-party doctrine, established by the Court in On Lee, Lopez, Lewis, and Hoffa, survive under the new Katz test? Indeed, Katz rejected limiting “searches” to instances of physical governmental intrusions, and instead adopted a more functional test that looks to an individual’s reasonable expectations of privacy. Might this mean that an individual could have a reasonable expectation of privacy in the content of a conversation with an undercover agent working for the government?

The Court unequivocally answered no in United States v. White, decided four years later. In White, the defendant discussed his illegal narcotics transactions with an undercover informant who was wearing a wire, and as in Lopez, the recordings were used against him at trial. Justice White’s plurality opinion explained that On Lee, Lopez, Lewis, and Hoffa would survive Katz. The Court stated:

64. Id.
65. Id.
66. Id. at 348–50.
68. Id. at 358–59.
69. Id. at 357.
70. Id. at 361 (Harlan, J., concurring).
72. 401 U.S. 745 (1971); Kerr, supra note 10, at 568.
73. White, 401 U.S. at 746–47.
74. Id. at 749–54; Kerr, supra note 10, at 568.
Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his. 75

In other words, under the *Katz* test, an individual has no reasonable expectation of privacy in information he voluntarily discloses to third parties.

3. Accountants, Banks, and Business Records

The Supreme Court subsequently expanded the third-party doctrine from secret agents to business records in a series of cases between 1973 and 1980. 76 In all of these cases, the Court held that an individual surrenders her Fourth Amendment rights when she transfers business records to a third party. 77 In *Couch v. United States*, the defendant turned over business and tax records to her accountant. 78 In connection with an investigation of the defendant’s tax liability, the government issued an IRS summons requiring the accountant to produce “[a]ll books, records, bank statements, cancelled checks, deposit ticket copies, workpapers and all other pertinent documents pertaining to the tax liability of the [defendant].” 79 The defendant intervened and moved to halt production of the records as evidence obtained in violation of the Fourth and Fifth Amendments. 80 The Court rejected her Fourth Amendment claim, holding that no “search” had occurred. 81 The Court explained that under *Katz*, “there can be little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return.” 82 Indeed, by turning over her information to her accountant, the defendant had given her accountant “the power to decide what information would be further disclosed in [her] income tax returns.” 83

Several years later, the Court was again confronted with the scope of the third-party doctrine in *United States v. Miller* 84 and then in *United States v. Payner*. 85 In *Miller*, the government served subpoenas on two banks where defendant Miller maintained accounts, requesting “all records of accounts, *i.e.*,...
savings, checking, loan or otherwise.”

Upholding admission of the bank records in *Miller*, the Court held that because the defendant had voluntarily turned over the bank records to a third party, he was not entitled to Fourth Amendment protection. Writing for the majority, Justice Powell explained that “[the defendant took] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government.” In *Payner*, investigators stole a briefcase owned by Michael Wolstencroft, vice president and trust officer of Castle Bank, Florida. The investigators then photographed over 400 documents found in the briefcase before returning it to Wolstencroft’s hotel room. The documents photographed included papers showing a close working relationship between the Castle Bank and the Bank of Perrine, Florida. The government subsequently served subpoenas to the Bank of Perrine and ultimately uncovered a loan guarantee agreement in which the defendant pledged funds in a foreign bank account at the Castle Bank and Trust Company of Nassau, Bahama Islands. This evidence enabled the government to prove that the defendant had “knowingly” falsified his tax return in violation of 18 U.S.C. § 1001 when he had denied maintaining a foreign bank account. The Court upheld admission of the loan agreement under the Fourth Amendment, concluding that the case was indistinguishable from *Miller*.

Thus, the Supreme Court had fashioned a sweeping Fourth Amendment doctrine, establishing that when an individual discloses information to a third party, he forfeits any reasonable expectation of privacy in it. The Court had found this doctrine to apply broadly, to cases in which a defendant has made damaging statements to an undercover agent, and to those in which he has turned over records to an accountant or bank.

87. *See id.* at 442–43; *Kerr, supra* note 10, at 569–70.
89. *Payner*, 447 U.S. at 730; *Kerr, supra* note 10, at 569.
91. *Id.*
92. *Id.* at 728, 730, 742.
93. *Id.* at 728, 730.
94. *Kerr, supra* note 10, at 570; *see Payner*, 447 U.S. at 732 (“United States v. Miller . . . established that a depositor has no expectation of privacy and thus no ‘protectable Fourth Amendment interest’ in copies of checks and deposit slips retained by his bank. . . . Nothing in the record supports a contrary conclusion in this case.”).
4. Pen Registers

Finally, in *Smith v. Maryland*, the Court expanded the third-party doctrine further, to numerical telephone information conveyed by a customer to his telephone company.98 In *Smith*, investigators suspected a man of robbing and then making threatening and obscene phone calls to a woman at her home.99 The telephone company, at the government’s request, installed a pen register,100 which recorded the numbers dialed from the suspect’s home for two days.101 The pen register “confirmed that the calls were originating from the man’s home, and that information was used to help get a warrant to search his home.”102

The Supreme Court held that the installation and use of the pen register did not constitute a “search” under the Fourth Amendment, and hence no warrant or probable cause was required to utilize it.103 The Court reasoned that under the *Katz* test, the defendant did not have a subjective expectation of privacy in the numbers he dialed, given that he was aware they would be conveyed to the telephone company to connect his call.104 And even if he did possess a subjective expectation of privacy, it was not one which society would be prepared to recognize as reasonable.105 In other words, the pen register was not a “search” because it was covered by the third-party doctrine. The Court explained that “[w]hen he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal the numbers he dialed.”106

*Smith* has been consistently followed by federal courts of appeals and some judges have extended the decision’s reasoning to more technologically sophisticated versions of the pen register, ruling that metadata is generally outside of

99. Id. at 737.
100. Id. The “pen register” was “a[n] [electronic] device installed at the phone company to record the numbers dialed from a specific telephone [line].” Kerr, supra note 10, at 570.
101. Smith, 442 U.S. at 737.
102. Kerr, supra note 10, at 570.
103. Smith, 442 U.S. at 745–46.
104. Id. at 742–43. (“[W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. . . . Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. . . . [I]t is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.”). The Court noted the limited capabilities of pen registers. Id. at 741. They do not hear sound, disclose only telephone numbers dialed, do not reveal whether a call was even completed, and do not reveal caller or recipient identities. Id.
105. Id. at 743–44. (“[E]ven if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not ‘one that society is prepared to recognize as ‘reasonable.’”).
106. Id. at 744.
Fourth Amendment protection. Again, it should be emphasized that the pen register at issue in *Smith* was quite rudimentary—it was, after all, 1979. The device targeted a single criminal defendant, was operational for a matter of days, and the government only retained the records collected until the case was over. While the device did reveal phone numbers dialed, date, and time, it did not reveal whether a call was completed or the duration of any call. By contrast, phone companies today collect and store subscribers’ telephony metadata on an on-going basis. The data collected is much more comprehensive, often including not only the numbers dialed, date, and time, but also the duration of each call and whether it was completed. And there is some evidence that telephony metadata can reveal a user’s location. Most importantly, the ubiquity of cell phones today has significantly altered the amount of information available to phone companies for a given customer. At the time of *Smith*, for example, metadata pertaining to “people trying to locate one another in a public space” simply did not exist. Despite this technological and cultural shift, the holding of *Smith* and its application to modern metadata collection went largely unquestioned. The Eighth Circuit, for example, unanimously held that the Fourth Amendment does not protect stored telephone records, while the Ninth Circuit expanded the third-party doctrine to the electronic age, concluding that the Fourth Amendment does not protect Internet metadata.

**C. Exposure to the Public At-Large: Aerial Surveillance and Curbside Trash**

As the Court expanded the third-party doctrine from secret agents to business records to pen registers, it also developed a parallel strand of jurisprudence expressing a broader principle: information exposed to the public at-large is also unprotected by the Fourth Amendment. This branch of the third-party doctrine

---


109. *Id.* at 35.

110. *Smith*, 442 U.S. at 741; see also *Klayman*, 957 F. Supp. 2d at 35 n.57.


113. *Id.*

114. *Id.* at 35–36.

115. *Id.* at 36.

116. United States v. Fregoso, 60 F.3d 1314, 1321 (8th Cir. 1995).

117. United States v. Forrester, 495 F.3d 1041, 1050 (9th Cir. 2007).
developed in two contexts: aerial surveillance\textsuperscript{118} and the collection of garbage left outside the curtilage of the home.\textsuperscript{119}

In \textit{Ciraolo}, without first obtaining a warrant, police officers secured an airplane, flew over the defendant’s residence at an altitude of 1,000 feet, and identified marijuana plants in his yard.\textsuperscript{120} On the basis of these naked-eye observations and photographs taken, the officers obtained a warrant, searched the premises, and seized marijuana plants.\textsuperscript{121} The Supreme Court was asked to determine whether the warrantless aerial surveillance constituted an unconstitutional Fourth Amendment “search.”\textsuperscript{122} In a 5-4 decision, the Court held that under \textit{Katz}, the government had not conducted a “search.”\textsuperscript{123} The Court reasoned that the defendant had “knowingly expose[d]” his backyard to aerial observation with the naked eye and “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”\textsuperscript{124} Indeed, “[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed,”\textsuperscript{125} and police officers cannot be expected “to shield their eyes.”\textsuperscript{126} The Court thus concluded that the defendant’s expectation that his garden was protected from aerial surveillance was unreasonable, drawing an analogy to the Court’s reflection in \textit{Katz} that “conversations in the open would not be protected against being overheard.”\textsuperscript{127}

The Court reaffirmed this principle several years later in \textit{California v. Greenwood}\textsuperscript{128} and \textit{Florida v. Riley}\textsuperscript{129} In \textit{Greenwood}, citing \textit{Ciraolo} and \textit{Smith}, the Court held that the Fourth Amendment does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of a home.\textsuperscript{130} In \textit{Riley}, which had similar facts to \textit{Ciraolo}, police officers engaged in naked-eye aerial

\begin{itemize}
\item \textsuperscript{118} California v. Ciraolo, 476 U.S. 207, 209 (1986).
\item \textsuperscript{119} California v. Greenwood, 486 U.S. 35, 37 (1988).
\item \textsuperscript{120} \textit{Ciraolo}, 476 U.S. at 209.
\item \textsuperscript{121} \textit{Id.} at 209–10.
\item \textsuperscript{122} \textit{Id.} at 209.
\item \textsuperscript{123} \textit{Id.} at 211–215.
\item \textsuperscript{124} \textit{Id.} at 213 (quoting \textit{Katz} v. United States, 389 U.S. 347, 351 (1967)).
\item \textsuperscript{125} \textit{Id.} at 213–14.
\item \textsuperscript{126} \textit{Id.} at 213.
\item \textsuperscript{127} \textit{Id.} at 215 (quoting \textit{Katz}, 389 U.S. at 361) (internal quotation marks omitted).
\item \textsuperscript{128} 486 U.S. 35 (1988).
\item \textsuperscript{129} 488 U.S. 445 (1989).
\item \textsuperscript{130} \textit{Greenwood}, 486 U.S. at 40–41. Writing for the majority, Justice White stated:
\end{itemize}

It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoopers, and other members of the public. Moreover, respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents’ trash or permitted others, such as the police, to do so. . . . [H]aving deposited their garbage ‘in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it; respondents could have had no reasonable expectation of privacy in the inculpatory items that they discarded. . . . [T]he police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the
surveillance of a partially covered greenhouse in a backyard. In contrast to Ciraolo, however, the officers used a helicopter instead of an airplane and hovered above the property at 400 rather than 1,000 feet. Citing Katz and Ciraolo, the Court held that the surveillance did not constitute a “search” for which a warrant was required under the Fourth Amendment. The majority explained that “[a]ny member of the public could legally have been flying over Riley’s property in a helicopter at the altitude of 400 feet and could have observed Riley’s greenhouse. The police officer did no more.”

II. THE FOURTH AMENDMENT IN THE CYBER AGE: BYTES SNEAKING OUT

With recent technological advantages, American society has undergone immense changes, which have impacted the third-party doctrine. First, we have seen the emergence of technologies enabling law enforcement to capture information exposed to the public, ordinarily not perceivable by human beings. Officers can use infrared scanners to capture heat signals and highly trained dogs to capture scents emanating from private homes or automobiles. A strict application of the third-party doctrine would tell us that using such technologies is not a Fourth Amendment “search,” because you do not have a reasonable expectation of privacy in information (including heat signals or scents) emanating from a home or automobile. To what extent, if at all, should these technologies impact our application of the third-party doctrine? Second, Americans, in their daily lives, disclose an unprecedented amount of information to third parties. This development has been fuelled by the information age and the rise of the Internet as an institution of modern life. We expose metadata not only to telephone companies, but also to Internet Service Providers (ISPs), web browsers, and online banking systems. We also voluntarily disclose detailed information about our private lives, including information about our age, sex, and religious views, to Facebook, Twitter, Snapchat, and LinkedIn in order to participate in digital social and political life.

The Supreme Court and lower federal courts have all taken notice, struggling to apply the third-party doctrine to these technological and societal developments. The underlying concern is that these immense changes might enable the third-party doctrine to usurp and displace the Fourth Amendment wholesale. Katz teaches us that police must obtain a warrant issued upon probable cause in order to conduct a search of a place in which an individual retains a reasonable expectation of public. Hence, “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”

Id. (quoting Katz, 389 U.S. at 351) (citations omitted).
132. Id.
133. Id. at 450–52.
134. Id. at 451.
of privacy. And the third-party doctrine, in its traditional form, operates as virtually a per se rule that any time an individual exposes information to another person or the public, he or she loses any expectation of privacy in it. Thus, in a world in which everyone exposes everything to third parties due to the central role of the Internet and in which technologies can capture previously undetectable private information exposed to the public at-large, the core protections afforded by the Fourth Amendment begin to erode. The third-party doctrine would serve as a way to circumvent our right “to be secure in [our] persons, houses, papers, and effects.”

Grappling with these doctrinal difficulties, the Supreme Court has begun to subtly push back against the third-party doctrine. Part A will analyze two cases, dealing with thermal imagers and hospital records, in which the Supreme Court first began to push back against the third-party doctrine. Part B will then examine the Court’s most recent third-party doctrine cases, particularly United States v. Jones, which provides the strongest indication that the Court might be prepared to abandon the third-party doctrine wholly or in part.

A. The Beginning of the End of the Third-Party Doctrine?: Thermal Imagers and Hospital Records

The Supreme Court first began to push back against the third-party doctrine in two cases both decided during the 2001 term. In Kyllo v. United States, the Court was asked to apply the third-party doctrine to the government’s use of thermal imagers to capture heat signals emanating from a home, while Ferguson v. City of Charleston dealt with a hospital’s disclosure of patient medical records to law enforcement officials. The Kyllo decision arguably represents a slight retreat from the Court’s public exposure line of cases, including Ciraolo and Riley, while Ferguson seems to depart from the rule established in Smith that business records disclosed to third-parties do not receive Fourth Amendment protection.

1. Thermal Imagers: Kyllo v. United States

The Supreme Court’s third-party doctrine can be broken down into two broad strands of jurisprudence. First is what might be called the Court’s “public exposure” jurisprudence, a series of cases dealing with the exposure of information, usually in or around the curtilage of the home, to the public at-large. These cases include Greenwood, Ciraolo, and Riley, discussed above. This branch of the third-party doctrine has traditionally expressed the principle that information

135. U.S. CONST. amend. IV.
139. Kyllo, 533 U.S. at 29.
140. Ferguson, 532 U.S. at 69–70.
voluntarily exposed from your home to the public at-large does not receive Fourth Amendment protection. Officers can permissibly fly overhead to engage in aerial surveillance, collect discarded trash left on your curb for pickup, or execute a twenty-four-hour “stakeout” of your building. Most importantly, officers can constitutionally do all of these things without probable cause or a warrant because, in the words of Justice Scalia, there simply “is no ‘search’ at all—perhaps in order to preserve somewhat more intact our doctrine that warrantless searches are presumptively unconstitutional.”141

What *Kyllo* is really about is whether this principle should change in circumstances where officers capture publicly exposed information, not through ordinary human sensory perception (sight, hearing, smell, or touch), but through the use of a new technology without which they would not be able to access the information. Indeed, *Kyllo v. United States*142 was the first time the Court attempted to apply the third-party doctrine to modern technology. *Kyllo* begins, as many of these stories do, with federal agents who suspected a defendant of growing marijuana in his home.143 Marijuana grown inside usually requires high-intensity lamps.144 In order to determine whether an amount of heat was emanating from the home indicating the use of such lamps, the agents used a thermal imager to scan the residence from the street.145 Such thermal imagers detect infrared radiation, which all objects emit but which is invisible to the naked human eye.146 The imager converts the radiation into images based on warmth with black representing cool and white indicating hot.147 The scan of the defendant’s home revealed that the garage roof and a side wall of the defendant’s house were relatively hot compared to the rest of the home and substantially warmer than neighboring homes.148 Agents concluded that the defendant was using halide lights to grow marijuana inside his home.149 Based on “tips from informants, utility bills, and the thermal imaging, a Federal Magistrate Judge issued a warrant authorizing a search of [the defendant’s] home” and the agents subsequently found an indoor marijuana growing operation inside the residence.150

The defendant moved to suppress the evidence of the marijuana growing operation found in his home as the fruit of an unconstitutional Fourth Amendment “search.”151 He asserted that the government’s use of the thermal imager was a

141. *Kyllo*, 533 U.S. at 32.
142. *Id.* at 27.
143. *Id.* at 29.
144. *Id.*
145. *Id.*
146. *Id.*
147. *Id.* at 29–30.
148. *Id.* at 30.
149. *Id.*
150. *Id.*
151. *Id.* at 30.
“search” for which a judicial warrant based on probable cause was required. At first glance, Kyllo would appear to require a simple application of the third-party doctrine as announced in Ciraolo and Riley. In those cases, the Court had held that aerial surveillance does not qualify as a “search” because citizens do not retain a reasonable expectation of privacy in information they have visually exposed to the public and officers should not be required to shield their eyes when passing by. Applying this principle here would seem to require a similar result: the government’s use of the thermal imager to scan the defendant’s home did not constitute a Fourth Amendment “search” because officers should not be expected to shield their eyes from heat emanating from a home. And, indeed, the Court of Appeals for the Ninth Circuit reached precisely this result after remanding the case to the district court for additional fact-finding. On remand, the district court had found that:

[The thermal imager was] a non-intrusive device which emits no rays or beams and shows a crude visual image of the heat being radiated from the outside of the house . . . [and] did not show any people or activity within the walls of the structure . . . [t]he device used cannot penetrate walls or windows to reveal conversations or human activities . . . and [n]o intimate details of the home were observed. Based on these factual findings, the Ninth Circuit affirmed the denial of the defendant’s motion to suppress. The court of appeals held that under Katz, the defendant had not demonstrated a subjective expectation of privacy because he did not attempt to conceal the heat emanating from his home. And even if he had manifested such an expectation of privacy, it was not one which society would be prepared to accept as reasonable because the thermal imager “did not expose any intimate details of [the defendant’s] life . . . only amorphous ‘hot spots’ on the roof and exterior wall.” This result makes sense given the third-party doctrine and the Court’s decisions in Ciraolo and Riley. But intuitively, it seems like it should matter that in Ciraolo and Riley the officers made naked-eye aerial observations, while in Kyllo, they made “thermal observations” using a new technology.

In overturning the Ninth Circuit’s decision in Kyllo, the Supreme Court’s majority opinion picked up on this subtle difference. The Court explained that what distinguished Kyllo from Ciraolo and Riley was that it involved officers on a
public street engaged in “more than naked-eye surveillance of a home.”\textsuperscript{159} According to the majority, while

“[the Court has] previously reserved judgment as to how much technological enhancement of ordinary perception from such a vantage point, if any, is too much . . . the question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.”\textsuperscript{160}

The Court proceeded to note how advances in technology had impacted the privacy protections of the Fourth Amendment, beginning with human flight, which “uncovered portions of the house and its curtilage that once were private.”\textsuperscript{161} To limit the detrimental impact of technology on the Fourth Amendment, the Court devised a novel test to be applied in cases involving surveillance of the home:

We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical “intrusion into a constitutionally protected area,” constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.\textsuperscript{162}

The Court, thus, concluded that the information obtained by the thermal imager was the product of a “search” under the Fourth Amendment.\textsuperscript{163} Thermal imagers enable police “to explore details of the home that would previously have been unknowable without physical intrusion” and they are technology not in general public use.\textsuperscript{164} The Court rejected the Government’s contention that the use of the thermal imager was permissible under the third-party doctrine because “it detected ‘only heat radiating from the external surface of the house.’”\textsuperscript{165} The Court explained that in \textit{Katz}, the eavesdropping device picked up only sound waves that reached the exterior of the phone booth and that “[r]eversing that approach would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home.”\textsuperscript{166}

The Court in \textit{Kyllo} seemed to say that it would not allow the Fourth Amendment to be eviscerated over time through a combination of technological advancement and the third-party doctrine. However, the problem with the test the Court devised is that by prohibiting police officers from using a particular technology only in instances where the device at issue is in “general public use,” the Court actually

\textsuperscript{159} Id. at 33 (emphasis added).
\textsuperscript{160} Id. at 33–34.
\textsuperscript{161} Id. at 34.
\textsuperscript{162} Id. (citation omitted).
\textsuperscript{163} Id. at 34–35.
\textsuperscript{164} Id. at 40.
\textsuperscript{165} Id. at 35.
\textsuperscript{166} Id. at 35–36.
subjected the Fourth Amendment to a slow demise by linking its “search” jurisprudence to technological advancement. To illustrate what I mean, once thermal imagers are in “general public use,” police will be able to use them to target homes without a warrant or probable cause. While this is a troubling consequence of *Kyllo*, it does seem consistent with the Court’s broader conception of the Fourth Amendment: in order to ferret out crime, police officers should be able to do anything that a private citizen could do. While *Kyllo* may have been the first case in which the Court pushed back against the third-party doctrine, it was certainly not the last.

2. Hospital Records: Ferguson v. City of Charleston

The next case, *Ferguson v. City of Charleston*,\(^{167}\) does not fall into the public exposure line of cases. It is not about the home, and it does not involve a novel technology; rather, it falls under the other branch of third-party doctrine. This branch includes a series of cases, which all involve secret agents\(^{168}\) or business records,\(^{169}\) and which express the principle that an individual does not retain a reasonable expectation of privacy in information turned over to third parties. Yet, *Ferguson* is significant precisely because it appears to be fundamentally in conflict with these cases. In *Ferguson*, staff members of the Charleston public hospital operated by the Medical University of South Carolina (“MUSC”) became concerned about an increase in the use of cocaine by obstetrics patients receiving prenatal treatment.\(^{170}\) To address the problem, a task force of MUSC representatives, police, and local officials designed a program which set forth procedures for identifying and testing pregnant patients suspected of drug use; required that a chain of custody be followed when obtaining and testing patients’ urine samples; provided for education and treatment referral for patients testing positive; contained police procedures and criteria for arresting patients who tested positive; and prescribed prosecutions for drug offenses and/or child neglect, depending on the stage of the defendant’s pregnancy.\(^{171}\)


\(^{170}\). *Ferguson*, 532 U.S. at 70.

\(^{171}\). *Id.* at 67.
In sum, an agreement was reached between the hospital and law enforcement, that MUSC would drug test prenatal patients and then turn the results over to the police without patients’ knowledge or consent.172

The defendants, MUSC prenatal patients arrested after testing positive for cocaine, filed suit challenging the program under the Fourth Amendment.173 The Court first addressed the question of whether the program entailed a “search” for which probable cause and a warrant were required under the Fourth Amendment.174 The majority held that “the urine tests conducted by those staff members were indisputably searches within the meaning of the Fourth Amendment.”175

Without much explanation as to why the government obtaining urine samples voluntarily turned over to a hospital as part of a medical treatment program should constitute a “search,” Justice Stevens simply noted that it has routinely treated urine tests taken by state agents as “searches” within the meaning of the Fourth Amendment.176 Noticing this major shortcoming, Justice Scalia filed a strongly worded dissent.177 In Justice Scalia’s view, no Fourth Amendment “search” had occurred under the facts of Ferguson, and he expressed frustration with the majority’s failure to explain their reasoning. Justice Scalia writes:

Until today, we have never held—or even suggested—that material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain. Without so much as discussing the point, the Court today opens a hole in our Fourth Amendment jurisprudence, the size and shape of which is entirely indeterminate. . . . Since the Court declines even to discuss the issue, it leaves law enforcement officials entirely in the dark as to when they can use incriminating evidence obtained from “trusted” sources. Presumably the lines will be drawn in the case-by-case development of a whole new branch of Fourth Amendment jurisprudence, taking yet another social judgment (which confidential relationships ought not be invaded by the police) out of democratic control, and confiding it to the uncontrolled judgment of this Court—uncontrolled because there is no common-law precedent to guide it. I would adhere to our established law, which says that information obtained through violation of a relationship of trust is obtained consensually, and is hence not a search.178

172. Id. at 70–73, 77.
173. Id. at 73.
174. Id. at 76–78.
175. Id. at 76 (emphasis added) (citation omitted). It is important to emphasize that the majority opinion does not at all rely on any statute, such as the Health Insurance Portability and Accountability Act (“HIPAA”).
177. Id. at 91–104 (Scalia, J., dissenting).
178. Id. at 95–96 (Scalia, J., dissenting) (emphasis added); see id. at 96 n.4 (Scalia, J., dissenting) (“In sum, I think it clear that the Court’s disposition requires the holding that violation of a relationship of trust constitutes a search.”).
Seeking to expose the shortcomings of the majority opinion, Justice Scalia examined the possible ways in which the drug-testing program might have entailed a Fourth Amendment "search." First, the hospital’s reporting of positive drug-test results to police is at most a "derivative use of the product of a past unlawful search, [which] work[s] no new Fourth Amendment wrong [and] presents a question, not of rights, but of remedies." Second, the testing of the urine for unlawful drugs might be regarded as a "search" of sorts. But, citing Greenwood, Justice Scalia concluded that urine cannot be regarded as an "effect" in instances where someone has abandoned it. In Justice Scalia’s view, then, the only act that could be regarded as a "search" was the actual taking of the urine sample. If the taking of the urine sample was forcible or coercive it might be deemed a "search," but if the taking of the sample was voluntary, it would not be. In Ferguson, however, the defendants did not assert that the urine samples were taken forcibly. Thus, the only basis for asserting that there had been a "search" was that the samples had been taken coercively without patients' consent in that (1) they were not told the tests would include testing for drugs; and (2) they were not told that the results of the tests would be provided to the police. However, citing the Court's "secret agent" cases Hoffa, White, and Miller, Justice Scalia explained that "lawfully (but deceivingly) obtain[ing] material for purposes other than those represented, and giving that material or information derived from it to the police, is not unconstitutional."

Having rejected these two bases of coercion, Justice Scalia turned to one final possibility: the patients’ consent to the hospital’s taking of their urine samples was coerced by the their need for the medical treatment of their pregnancy. However, Justice Scalia concluded "[i]f that was coercion, it was not coercion applied by the government—and if such nongovernmental coercion sufficed, the police would never be permitted to use the ballistic evidence obtained from

179. Id. at 92–93 (Scalia, J., dissenting).
181. Id. at 92 (Scalia, J., dissenting).
182. Id. at 92 (Scalia, J., dissenting) (citing California v. Greenwood, 486 U.S. 35 (1988) (holding that garbage left at the curb is not property protected by the Fourth Amendment)).
183. Id. at 92 (Scalia, J., dissenting).
184. Id. at 93 (Scalia, J., dissenting).
185. Id. (Scalia, J., dissenting).
186. Id. at 94 (Scalia, J., dissenting). “[T]he Fourth Amendment [does not protect] a wrongdoer’s misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it. Because the defendant had voluntarily provided access to the evidence, there was no reasonable expectation of privacy to invade.” Id. (Scalia, J., dissenting) (quoting Hoffa v. United States, 385 U.S. 293, 302 (1966) (internal quotation marks omitted)). “[H]owever strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment when it turns out that the colleague is a government agent regularly communicating with the authorities.” Id. (Scalia, J., dissenting) (quoting United States v. White, 401 U.S. 745, 749 (1971)) (internal quotation marks omitted).
187. Id. at 97 (Scalia, J., dissenting).
treatment of a patient with a bullet wound.” Justice Scalia seems right. At the very least Ferguson is in serious tension with Smith, Couch, Miller, and Hoffa. A plain reading of the Ferguson majority opinion suggests that in giving their urine to MUSC for diagnostic testing, the prenatal patients retained a reasonable expectation that it would not be used for drug testing, and that it would not be turned over to the police. As a consequence, a Fourth Amendment “search” occurred either when the hospital collected the urine, tested it for drugs, or transmitted positive results to law enforcement without patients’ consent. Justice Scalia persuasively argued that Ferguson represents a significant departure from the third-party doctrine. Indeed, is urine voluntarily turned over to a hospital really any different from tax documents turned over to a bank or metadata transmitted to the phone company? Alternatively, the opinion could be read as establishing some kind of exception to the Smith rule due to the uniquely private nature of medical records, particularly those involving obstetrics patients.

B. Recent Jurisprudence: Dog Sniffs and GPS Tracking

This Part will examine the Supreme Court’s two most recent decisions addressing the third-party doctrine: United States v. Maynard189 (reviewed by the Supreme Court as United States v. Jones190) and Florida v. Jardines.191 In both cases, the Court reaffirmed its position, first developed in Kyllo and Ferguson, that an individual can sometimes retain a reasonable expectation of privacy in information exposed to a third party or the public. Jones, in particular, hints that the Court might be prepared to cast aside the third-party doctrine given the realities of the cyber age, and replace it with a more nuanced and privacy-conducive conception of the Fourth Amendment.

In Maynard, police officers installed a Global Positioning System (“GPS”) tracking device on a Jeep owned by defendant Jones, which “established the vehicle’s location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer. It relayed more than 2,000 pages of data over the 4-week period.”192 One question presented to the United States Court of Appeals for the District of Columbia Circuit was whether installation of the device and collection of the GPS data over four weeks constituted a “search” for which a warrant and probable cause were required under the Fourth Amendment.193 If the D.C. Circuit had opted to strictly apply the third-party doctrine, Maynard would have been an easy case. The Fourth Amendment does not protect information voluntarily exposed to the public at-large, so the argument goes, and for that

188. Id. (Scalia, J., dissenting).
189. 615 F.3d 544 (D.C. Cir. 2010).
190. 132 S. Ct. 945 (2012).
193. Maynard, 615 F.3d at 549, 555.
reason, officers have always been able to follow suspects without probable cause or a warrant. Tailing a suspect is one of the most basic tools available to police officers, particularly where they do not have any other leads. And because “[t]he police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public,” when police obtained the defendant’s public movements there simply was no Fourth Amendment “search.”

Rejecting this approach, the D.C. Circuit held that the GPS tracking over the course of the month violated the defendant’s reasonable expectations of privacy, and thus constituted a “search” under Katz. Perceiving the unsuitability of the third-party doctrine to the cyber age, the D.C. Circuit adopted a novel “mosaic theory” of the Fourth Amendment. Under mosaic theory, whether a “search” has occurred is not determined by looking solely at the governmental conduct in individual steps, but rather by asking, “whether a series of acts that are not searches in isolation amount to a search when considered as a group.” In other words, a series of non-searches in aggregation can amount to a Fourth Amendment “search” because their collection and analysis generates a revealing “mosaic” about an individual. In this case, although the individual readings of the GPS device revealed information exposed to the public, the collective unit of the twenty-eight days of surveillance was not exposed to the public. This was the case because the aggregate sum of twenty-eight days of surveillance disclosed more than the sum of its parts. When put together, the discreet and individual non-searches became a “search” because they could be combined to form “a mosaic to reveal a full picture of a person’s life.” The government’s collection of this non-sequential “mosaic” violated the defendant’s reasonable expectation of privacy under Katz.

The Supreme Court later reviewed Maynard as United States v. Jones. The majority held that the installation of the GPS device and the collection of location

---

195. Maynard, 615 F.3d at 563.
197. Kerr, Mosaic Theory, supra note 196, at 320.
198. Id.
199. Maynard, 615 F.3d at 561–62.
200. Id. at 562 (“Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one’s not visiting any of these places over the course of a month. The sequence of a person’s movements can reveal still more: a single trip to a gynecologist’s office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.”).
201. See Kerr, Mosaic Theory, supra note 196, at 325.
data over the course of one month constituted a “search,” but relied on a physical trespass concept rather than the *Katz* test.\(^{203}\) However, five Justices of the Court appear ready to embrace the D.C. Circuit’s novel “mosaic theory”: Justices Ginsburg, Breyer, Alito, Kagan, and Sotomayor.\(^{204}\) Justice Alito filed a concurring opinion, with Justices Ginsburg, Breyer, and Kagan joining, arguing that the month-long GPS monitoring constituted a “search” under *Katz*.\(^{205}\) Justice Sotomayor likewise concurred, arguing that the installation of the GPS device might constitute a “search” even under *Katz*.\(^{206}\) She reasoned that the tracking of an individual’s movements voluntarily exposed to the public, over a long period of time, could violate a reasonable expectation of privacy.\(^{207}\) More fundamentally, Justice Sotomayor indicated a willingness to clearly overrule *Smith*.

It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I 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.\(^{208}\)

As a majority of the Supreme Court articulated in *Jones*, the mere fact that an individual has voluntarily shared information with a third party or the public does mean that they do not retain a reasonable expectation of privacy in it. Earlier I discussed the two doctrinal branches of the third-party doctrine. One involves the disclosure of information to a specific third party such as a bank or telephone company and the other involves disclosure of information to the public at-large. *Jones* falls into the public exposure line of cases. It is about whether the government’s use of a particular technology (a GPS device) demands that we set

\(^{203}\) *Id.* at 949.

\(^{204}\) See United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment); *id.* at 956 (Sotomayor, J., concurring); see also Kerr, *Mosaic Theory*, supra note 196, at 313.

\(^{205}\) *Id.* at 962–63 (Alito, J., concurring).

\(^{206}\) *Id.* at 954–57 (Sotomayor, J., concurring).

\(^{207}\) *Id.* at 956–57.

\(^{208}\) *Id.* at 957 (citations omitted).
aside the usual rule that information exposed to the public receives no Fourth Amendment protection. In that regard, *Jones* is most doctrinally similar to *Kyllo*, which similarly asked whether the government’s use of an infrared scanner should preclude application of the third-party doctrine.

In *Kyllo*, the Court developed a novel test, which looked to whether the technology at issue is in “general public use.” What is striking about *Jones* is that neither the majority opinion in *Maynard* nor the concurring opinions in *Jones* invoked the *Kyllo* test to determine whether GPS tracking devices were in “general public use.” Instead, they simply applied the *Katz* test minus the traditional rule that there can never be a reasonable expectation of privacy in information exposed to the public. It is uncontroversial that citizens can and do have subjective actual expectations of privacy in their public movements over the course of one-month. However, the significant development in *Jones* is that five justices held that under the *Katz* test, these subjective expectations of privacy in public movements could be objectively reasonable, despite the fact that a long line of third-party doctrine precedent suggests otherwise. Thus, *Jones* seems to indicate that in circumstances involving the government’s bulk collection and analysis of information exposed to the public over a long period of time, it might be prepared to recognize an expectation of privacy as objectively reasonable.

One year later, in *Florida v. Jardines*, the Court was again confronted with a difficult case involving the application of the third-party doctrine to a quasi-novel technology. In that case, officers led a highly trained drug-dog onto the front porch of a house without obtaining a warrant. The dog alerted to drugs and on the basis of that information, the officers obtained a search warrant. The Court concluded that the dog sniff was a “search” and held that when a police officer physically intrudes into a constitutionally protected area with the objective purpose of searching for contraband, there has been a “search.”

This was the case even though the trained drug dog was merely capturing smells, which were emanating from the defendant’s home to the public at-large. Justice Scalia, writing for the majority, explained that a private citizen has an implied license to enter the curtilage of the home to sell Girl Scout Cookies, deliver mail, or engage in other permissible activities. However, this implied license has limitations—strangers may not wander into the backyard of the home or sit on the porch for hours reading. A police officer likewise has an implied license to approach the home for limited purposes such as for a “knock and

---

210. *Id.* at 1413.
211. *Id.*
212. *Id.* at 1417–18.
213. *Id.* at 1415.
214. *Id.* at 1416–17.
talk.” Yet, as with private citizens, police officers’ implied license has limitations. Police officers may not physically intrude into the curtilage of a home with an objective purpose of searching for contraband. And the only possible purpose for bringing a trained drug-dog onto the front porch of a home would be to search for drugs.

Thus, *Jardines* stands as just the most recent example in a recent series of Supreme Court cases beginning with *Kyllo* and *Ferguson* and ending with *Jones* and *Jardines*, standing for the proposition that an individual can retain a reasonable expectation of privacy in information exposed to third parties or the public.

III. BACK TO THE FUTURE: THE NSA’S BULK TELEPHONY METADATA PROGRAM

This Section will argue that under existing Supreme Court precedent, the NSA’s bulk collection of telephony metadata constitutes a “search” for which a warrant and probable cause are required under the Fourth Amendment. Part A will provide background information on the NSA program. Part B will then analyze two recent conflicting district court opinions addressing the constitutionality of the NSA program. I conclude that Judge Leon of United States District Court for the District of Columbia got the better of the argument in *Klayman v. Obama*, holding that the NSA’s bulk collection of telephony metadata constitutes a “search” under the Fourth Amendment.

A. Background on the NSA Metadata Program

In June 2013, *The Guardian* newspaper began publishing classified NSA documents that had been acquired by Edward Snowden, a former system administrator at contractor Booz Allen Hamilton. Over the next five months, *The Guardian* revealed the existence of a variety of surveillance programs, including: the NSA’s bulk telephony metadata program, and Internet surveillance programs including PRISM, Project Chess, Tempura, ShellTrumpet, and XKeyscore. The remainder of this note will focus on the NSA’s bulk telephony metadata program, the existence of which was revealed when *The Guardian* leaked a previously secret order (“Verizon Order”) from the Foreign Intelligence Surveillance Act (“FISA”)

---

216. See id. at 1416–17.
217. Id.
218. Id.
220. Greenwald, supra note 1; Greenwald, MacAskill & Poitras, supra note 2; Reitman, supra note 2.
Court ("FISC").

“Metadata includes information about a phone call—who, where, when, and how long—but not the content of the conversation.”

Pursuant to Section 215 of the USA PATRIOT Act, the FISC order to Verizon required Verizon to produce to the NSA:

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 . . . Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.

Following this disclosure, the government corroborated the authenticity of the document, and intelligence officials and leaders of the congressional committees confirmed that the leaked order was part of an ongoing metadata surveillance program that began in 2006.

In sum, the metadata collected under the NSA program includes the telephone numbers placing and receiving calls and the date,
time, and duration of those calls.\footnote{228}{See David S. Kris, On the Bulk Collection of Tangible Things, 1.4 LAWFARE RES. PAPER SERIES 1, 2–3 (2013), available at http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf.} It does not include the content of conversations,\footnote{229}{See OBAMA WHITE PAPER, supra note 11, at 1.} customers’ identities, or their physical locations.\footnote{230}{See Kris, supra note 228, at 3.} Although at the time of the initial disclosure, it was not known whether Verizon was the only company subject to bulk orders under Section 215, two days later The Wall Street Journal reported that the NSA had regularly obtained bulk metadata from the three major American telephone companies: Verizon, AT&T, and Sprint.\footnote{231}{Gorman et al., supra note 111.} It was estimated that this amounted to the metadata for several billion calls per day\footnote{232}{See Jonathan Stray, FAQ: What You Need to Know About the NSA’s Surveillance Programs, PROPUBLICA (Aug. 5, 2013), http://www.propublica.org/article/nsa-data-collection-faq.} and that every time most Americans placed a telephone call, the NSA obtained their metadata.\footnote{233}{See, e.g., Gorman et al., supra note 111.} This turned out to be somewhat of an overstatement, as in February 2014, it was disclosed that the actual percentage of records gathered under the program was somewhere between twenty percent and thirty percent of Americans’ calls.\footnote{234}{Ellen Nakashima, NSA is Collecting Less Than 30 Percent of U.S. Call Data, Officials Say, WASH. POST (Feb. 7, 2014), http://www.washingtonpost.com/world/national-security/nsa-is-collecting-less-than-30-percent-of-us-call-data-officials-say/2014/02/07/234a0e9e-8fad-11e3-b46a-5a3d0d2130da_story.html.} However, “[t]hat low percentage still probably represents tens of billions of records going back five years.”\footnote{235}{Id. (emphasis added).}

Once the telephony metadata is transmitted to the NSA, it is heavily restricted pursuant to procedures established in each order by the FISC.\footnote{236}{See Bradbury, supra note 227, at 2–4.} The metadata is stored for five years in a database,\footnote{237}{See Kris, supra note 228, at 15. Non-queried telephony metadata is deleted on a rolling basis and metadata found to have been inappropriately gathered is destroyed. Id.} which cannot be randomly accessed or searched.\footnote{238}{Id. at 2–3.} Rather, NSA analysts may only access the database to search (“query”) a particular phone number (“seed number”).\footnote{239}{See Kris, supra note 228, at 11. A finding of reasonable articulable suspicion justifying a query “must be made initially by one of 22 persons at NSA (20 line personnel and two supervisors), and all queries appear to require approvals from at least two persons before being implemented.” Id.} In order to conduct a query, a designated NSA official\footnote{240}{Id. at 2–3.} must determine that there is a reasonable, articulable suspicion that the seed number is associated with one of several designated terrorist organizations.\footnote{241}{Id. at 10; see also Primary Order at 7–9, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-80 (FISA Apr. 25, 2013), available at http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf. Officials are prohibited from querying a seed number for “any other foreign intelligence purpose, such as counter espionage.” Kris, supra note 228.} In addition, if the phone number appears to be a U.S. number, the reasonable suspicion cannot be based exclusively on
activities protected by the First Amendment. Conducting a query produces a list of any numbers that have been called from the seed number or that have called it and the time and duration of those connections. NSA officials are also permitted to analyze the metadata through “three-hop network analysis.” Every call that a suspect makes counts as a “hop,” while each call those recipients make is an additional hop. According to NSA Deputy Director Chris Inglis, the NSA “conducts three-hop network analysis—that is, it analyzes data up to three degrees of separation from initial terrorist suspects.” Therefore, if an individual “has forty contacts, three-hop network analysis could encompass data relating to 2.5 million people.”

Last, the FISC requires that the government adhere to court-monitored minimization procedures to reduce dissemination of queried U.S. phone numbers outside of the NSA. Thus, when a query leads to information, which relates to an American citizen, one of eleven designated NSA officials must give their approval before the information may be disseminated to other agencies. And approval for dissemination outside of the NSA will only be granted if the information “pertains to counterterrorism and is necessary to understand counterterrorism information, or assess its importance.” In addition to FISC oversight, the program is “subject to after-the-fact auditing and review by other entities within the Executive Branch and Congress.” The FISC has also been concerned about serious compliance issues surrounding the program, and has

228, at 10. At some point, the NSA must submit to the FISC a specific list of terrorist organizations to which a seed number may relate, which the court approves. Id.

242. See Bradbury, supra note 227, at 2.
243. Id. at 3.
244. See id.; Mornin, supra note 223, at 995.
245. Mornin, supra note 223, at 995.
247. Id.
248. See Bradbury, supra note 227, at 3.
249. See Kris, supra note 228, at 14.
250. Id.
251. Id. at 11.
252. See Bradbury, supra note 227, at 3 (“FISA mandates periodic audits by inspectors general and reporting to the Intelligence and Judiciary Committees of Congress. When section 215 was reauthorized in 2011, the administration briefed the leaders of Congress and the members of these Committees on the details of this program.”).
253. See Kris, supra note 228, at 16 n.62 (discussing the variety of NSA infractions under the program, including “(1) improper automated querying of the incoming metadata with non-RAS approved selectors; (2) inadvertent manual queries of the metadata using 14 non-RAS approved selectors by 3 analysts over a period of approximately 11 weeks; (3) omitting the required review by NSA’s Office of General Counsel of approximately 3,000 RAS determinations between 2006 and 2009; (4) failure to audit a database of query results; (5) using telephony metadata selectors identified by data integrity analysts as not appropriate for follow-up investigation to populate similar kinds of defeat lists in other NSA databases; (6) treating as RAS-approved all selectors associated with a particular person when any selector associated with that person is RAS-approved; (7) sharing
issued several rebukes to the NSA and added additional restrictions.\textsuperscript{254}

\textbf{B. The End of Smith v. Maryland?}

This Part explore whether the NSA’s bulk collection of telephony metadata constitutes a “search” under the Fourth Amendment. Subpart 1 will analyze the holdings of two federal district judges concerning the constitutionality of the NSA program. Subpart 2 will then argue that Judge Leon on the United States District Court for the District of Columbia got the better of the argument in \textit{Klayman v. Obama}\textsuperscript{255} and that if it is asked to review the NSA program, the Supreme Court should follow its recent trend in cases like \textit{Ferguson}, \textit{Jones}, and \textit{Jardines} and hold that the NSA’s bulk collection of telephony metadata constitutes a “search” under the Fourth Amendment.

\textit{1. A Tale of Two Cities}

The next legal issue is whether the NSA’s bulk collection of telephony metadata constitutes a “search” under the Fourth Amendment. Recently in \textit{ACLU v. Clapper}, the United States District Court for the Southern District of New York sided with the Obama Administration and ruled that the NSA’s bulk collection does not qualify as a Fourth Amendment “search.”\textsuperscript{256} The ACLU had filed suit against the NSA in federal district court in Manhattan one week after The Guardian published the Verizon Order, alleging that the NSA’s bulk telephony metadata program violated the organization’s Fourth Amendment rights.\textsuperscript{257} After briefing and oral argument, Judge William H. Pauley III rejected the ACLU’s motion for a preliminary injunction and granted the government’s motion to dismiss the complaint.\textsuperscript{258} Identifying \textit{Smith} as clear and controlling precedent, the court held that because “a subscriber has no legitimate expectation of privacy in telephony metadata created by third parties,” the NSA’s bulk collection of telephony metadata does not constitute a “search” under the Fourth Amendment.\textsuperscript{259} Judge Pauley III explained that the NSA’s collection of “breathtaking amounts” of unprotected information under the Fourth Amendment does not transform that

\begin{itemize}
\item query results with 98\% of NSA analysts not authorized to access the metadata database; (8) acquisition of metadata for foreign-to-foreign telephone calls from a provider that believed such metadata to be within the scope of the FISC’s order, when it was not; (9) failure to conduct the required OGC review for certain RAS findings; (10) mistaken inclusion of unminimized query results in a database available to analysis from other U.S. intelligence agencies; (11) sharing of query results without the required approvals; and (12) dissemination of query results to NSA analysts who had not received the proper training” (citations omitted)).
\end{itemize}

\textsuperscript{254}. See Kris, \textit{supra} note 228, at 17. The government maintains that none of its compliance infractions have been intentional or in bad-faith and that since 2009, none involved application of the reasonable articulable suspicion standard. \textit{Id.}


\textsuperscript{256}. 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013).

\textsuperscript{257}. \textit{Id.} at 735.

\textsuperscript{258}. \textit{Id.} at 757.

\textsuperscript{259}. \textit{Id.} at 752.
sweep into a Fourth Amendment “search.”260 In addition, he reasoned that “what metadata is has not changed over time,” and “[a]s in Smith, the types of information at issue . . . are relatively limited: [tele]phone numbers dialed, date, time, and the like.”261 Finally, the court acknowledged the five concurring opinions in Jones,262 but asserted that “the Supreme Court did not overrule Smith” in that case.263 Despite this trivial reference to Jones, Judge Pauley III all but ignored the vast majority of the Supreme Court’s recent third-party doctrine jurisprudence.264

Yet, Judge Pauley III is only the most recent sitting federal judge to rule on the constitutionality of the NSA’s bulk telephony metadata program. Ten days before Judge Pauley III issued his opinion, Judge Richard Leon on the United States District Court for the District of Columbia had come to the opposite conclusion in Klayman v. Obama.265 Contrary to Judge Pauley III, Judge Leon concluded that the NSA’s bulk collection of telephony metadata constitutes a “search” under the Fourth Amendment.266 Judge Leon observed that this case was a far cry from the installation and use of a single pen register in Smith v. Maryland.267 For that reason, he reframed the question presented as “[w]hen do present-day circumstances—the evolutions in the Government’s surveillance capabilities, citizens’ phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like Smith simply does not apply?”268 The answer, according to Judge Leon, is now.269

Although conceding that “what metadata is has not changed over time” and “the types of information at issue in this case are relatively limited,”270 Judge Leon proceeded to advance four main arguments as to why the NSA’s bulk collection of

260. Id. at 752 (citing United States v. Dionisio, 410 U.S. 1, 13, 93 (1973); In re Grand Jury Proceedings: Subpoenas Duces Tecum, 827 F.2d 301, 305 (8th Cir. 1987) (“[T]he fourth amendment does not necessarily prohibit the grand jury from engaging in a ‘dragnet’ operation.”)).

261. Id. (alteration in original) (footnotes omitted)

262. Id.; see United States v. Jones, 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring); id. at 956 (Sotomayor, J., concurring); see also Kerr, Mosaic Theory, supra note 196, at 313.

263. ACLU, 959 F. Supp. 2d at 752 (“[T]he Court of Appeals . . . leave[e] to th[e Supreme] Court the prerogative of overruling its own decisions.” (citing Agostini v. Felton, 521 U.S. 203, 237 (1997) (internal quotation marks omitted))).


266. Id. at 30.

267. Id. at 31.

268. Id.

269. Id.

270. Id. at 35 (emphasis omitted).
telephony metadata is a “search.” First, citing extensively to Jones and Maynard, he explained that short-range, short-term tracking devices differ significantly from constant, long-term tracking devices. As the concurring justices explained in Jones, while a person has no reasonable expectation of privacy in their short-term public movements, “the longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.” Analogizing, the pen register at issue in Smith was only operational for two days, and there was “no indication . . . that it expected the Government to retain those limited phone records once the case was over.” By contrast, the NSA’s telephony metadata program involves the creation and maintenance of a long-term historical database containing five years worth of metadata, which could conceivably go on forever. Second, while in Smith, police made a single request to install a pen register, “[u]nder this program . . . certain telecommunications service providers [ ] produce to the NSA on a daily basis electronic copies of call detail records, or telephony metadata.” Third, the advanced technology that enables the government to store and analyze the metadata of every telephone user in the United States for five years would have been inconceivable in 1979. And finally, “the nature and quantity of the information contained in people’s telephony metadata is much greater.”

271. Id. at 32–37.
272. Id. at 32.
273. Id. at 31.
274. Id. at 32.
275. See id. at 32.
276. Id. at 32 (citations omitted) (internal quotation marks omitted).

The Supreme Court itself has long-recognized 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, with the latter raising Fourth Amendment concerns.

Id. at 33 (emphasis added) (citations omitted).

277. Id. at 33.
278. Id. at 33–34. Judge Leon writes:

The number of mobile subscribers in 2013 is more than 3,000 times greater than the 91,600 subscriber connections in 1984, and more than triple the 97,035,925 subscribers in June 2000. It is now safe to assume that the vast majority of people reading this opinion have at least one cell phone within arm’s reach . . . . Thirty-four years ago, none of those phones would have been there. Thirty-four years ago, city streets were lined with pay phones. Thirty-four years ago, when people wanted to send “text messages,” they wrote letters and attached postage stamps.

Id. at 34–35 (citations omitted).
The Obama Administration in *Klayman* and the plaintiffs in *ACLU v. Clapper* have appealed to the D.C. Circuit and the Second Circuit respectively. On September 2, 2014, the U.S. government defended the NSA program before a “skeptical” Second Circuit panel in *ACLU v. Clapper*, but the court has yet to issue a ruling. The D.C. Circuit, likewise, heard oral argument in *Klayman* on November 4, 2014. While Judge Stephen Williams of the D.C. Circuit appeared to agree with the government, Judge Janice Rogers Brown, referencing *Ferguson*, noted that in a case “involving medical records . . . the Supreme Court ruled that people have privacy rights in data about them held by a hospital.”

With a split between two well-respected federal district courts, and a question of national importance at issue, the stakes cannot be overstated. Regardless of the outcome, by early 2015, there will be two published federal appellate rulings addressing the constitutionality of the NSA’s bulk telephony metadata program. Particularly if the D.C. Circuit and the Second Circuit issue conflicting opinions, the question of whether the NSA’s bulk collection of telephony metadata constitutes a “search” will most likely end up at the Supreme Court. And unlike in *Jones*, the Court will not have the option of relying on “trespass analysis” to avoid directly addressing the viability of *Smith* and the third-party doctrine. The next section will argue that the Supreme Court should follow its recent trend in decisions like *Jones* and hold that the NSA’s bulk collection of telephony metadata constitutes a “search.”

2. Judge Leon Got It “Mostly” Right: The NSA’s Bulk Collection of Telephony Metadata Constitutes a “Search” Under the Fourth Amendment

As an initial starting point, Judge Pauley III was correct that Fourth Amendment rights are indeed individual rights. As the Supreme Court explained in *United States v. Dionisio*, where a single grand jury subpoena did not constitute a Fourth Amendment “seizure,” it could not be “rendered unreasonable by the fact that many others were subjected to the same compulsion.” For that reason, the fact that the NSA program targets millions of Americans is immaterial to whether the program violates the Fourth Amendment. While the vastness of the program is

---


283. 410 U.S. 1, 13 (1973).
shocking and troubling, any constitutional analysis must necessarily focus on individual Fourth Amendment rights. Judge Pauley III in ACLU v. Clapper recognized this principle perhaps more so than Judge Leon did in Klayman, but ultimately, Judge Leon’s analysis more accurately captures the drift of Supreme Court precedent. The facts of Smith at first seem strikingly similar to the NSA’s bulk telephony metadata program, and Judge Pauley III was right in so far as Smith remains binding legal precedent. However, the Supreme Court develops the law over time by clarifying, limiting, and applying it to new circumstances. In Smith, the Court plainly held that under the Katz test, an individual does not retain a reasonable expectation of privacy in two days of telephony metadata turned over to the telephone company.284 However, while Smith might remain good law in cases concerning small amounts of telephony metadata, the Court has never addressed the constitutionality of the government’s long-term acquisition and aggregation of telephony metadata.

The NSA program systematically collects individuals’ telephony metadata on an ongoing and daily basis. The Supreme Court has never upheld this kind of long-term technological dragnet under the third-party doctrine. In fact, United States v. Jones is the only case in which the Court directly confronted long-term data collection, and in that case, it opted to strike down the government’s tracking of the defendant’s public movements over one month using GPS.285 But before there was Jones, there was United States v. Knotts,286 and an understanding of the Court’s transition between these two cases is essential to grasping what is going on in the NSA litigation. In Knotts, the Court had held that the government’s use of short-term, short-range GPS tracking devices did not constitute a “search.”287 Almost thirty years later, in Jones, which dealt with long-term, long-range GPS tracking, the government understandably asserted that Knotts was directly on point.288 The majority struck down the program on a trespass theory, but the five-justice plurality explained that while a person has no reasonable expectation of privacy in short-term public movements, they do have a reasonable expectation that the government will not subject them to GPS tracking over a period of twenty-eight days.289 The long-term nature of the surveillance turned out to be decisive. The Court’s holding changed in Jones because the facts changed. The government’s argument that Jones was Knotts “round two” fell on deaf ears. And in the same way that Knotts did not address the circumstances of Jones, Smith did not address the circumstances of the NSA program at issue in Klayman and ACLU v. Clapper.

287. Id. at 284–85.
289. Id. at 964 (Alito, J., concurring in judgment); id. at 956 (Sotomayor, J., concurring).
In *Smith*, the Court held that the government’s use of a single short-term pen register did not constitute a “search,” and the government now asserts that *Smith* is directly on point. But unlike in *Smith*, the NSA program systematically collects individuals’ metadata on an ongoing and daily basis and stores it in a computer system for five years. While the collection of a small amount of metadata might not be a “search,” in systematically collecting and storing individuals’ metadata over a long period of time, the NSA’s conduct was transformed from a series of non-searches into a collective Fourth Amendment search. The aggregate sum of five years of metadata, like the twenty-eight days of GPS surveillance data in *Jones*, “reveal[s] more than the sum of its parts” and can be combined to form “a mosaic to reveal the full picture of a person’s life.” By collecting and analyzing long-term metadata, the NSA obtains a complex picture of an individual’s religious, social, familial, and political affiliations on a level not revealed by smaller amounts of metadata. It is also not simply that the government collects individuals’ telephony metadata over a long period of time, but that the NSA also retains the information for storage and future querying. As Judge Leon correctly pointed out in *Klayman*, the pen register utilized in *Smith* was only operational for two days, and there was “no indication . . . that it expected the Government to retain those limited phone records once the case was over.” By contrast, the NSA’s telephony metadata program involves the creation and maintenance of a long-term historical database containing five years of data. This long-term collection violates individuals’ reasonable expectation of privacy under *Katz* and is a “search” under the Fourth Amendment.

While *Jones* serves as a starting point, *Ferguson v. City of Charleston* is the most underestimated recent Supreme Court case, which bears on the constitutionality of the NSA program. In *Ferguson*, the Court issued a majority opinion, which directly conflicts with *Smith*. The logic of *Ferguson* cannot help but lead to the conclusion that the NSA’s bulk collection of telephony metadata is likely a “search.” Other than a minor reference in Judge Leon’s opinion, *Ferguson* has

---

291. See Kerr, Mosaic Theory, supra note 196, at 325. Under the NSA program, metadata records collected do not identify the individuals or organizations associated with responsive telephone numbers. Thus, it might be asserted that the privacy interests at stake are minimal. However, whether a governmental intrusion constitutes an unconstitutional Fourth Amendment “search” does not turn on whether the police are aware of the identity of the individual whose home is “searched.” If officers were to follow a stranger to her home and unconstitutionally search her residence, the their lack of knowledge of her identity would not justify the impermissible intrusion. In other words, an individual’s reasonable expectation of privacy does not depend on whether police know her identity. Here, citizens either do or do not have a reasonable expectation of privacy in their telephony metadata. That fact that NSA officials do not have names or identities corresponding to phone numbers is irrelevant to the constitutional analysis.
292. See id.
295. See Klayman, 957 F. Supp. 2d at 33.
been surprisingly absent from the legal scholarship surrounding the NSA program and the litigation in Klayman and ACLU v. Clapper. One reason might be that Ferguson is largely known as a “special needs” case, and it is one of the few instances in which the Court found that a “special needs” program did not have a special programmatic purpose beyond the traditional need for crime control.296 But before the Court could conduct its “special needs” analysis in Ferguson, it first had to determine whether the government had engaged in a “search.”

To review the facts, in Ferguson, a hospital was concerned about an increase in cocaine use by obstetrics patients obtaining prenatal care.297 To address the problem, it established a formalized program in coordination with police, in which the hospital would test patients’ urine samples for cocaine.298 The test results were then turned over to law enforcement officials without the knowledge or consent of the patients, and a number of women were subsequently arrested or forced into treatment programs.299 The Court held this procedure entailed a Fourth Amendment “search.”300 As mentioned in Section II, Justice Scalia was greatly concerned that “[u]ntil today, we have never held—or even suggested—that material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain.”301 Indeed, a plain reading of Ferguson, would suggest that perhaps Judge Pauley III’s contention in ACLU v. Clapper that the “the Supreme Court did not overrule Smith [in Jones]”302 was correct. Instead, the Court limited Smith more than ten years ago in Ferguson.

Under this reading of Ferguson, the NSA’s bulk collection of telephony metadata constitutes a Fourth Amendment “search.” Americans voluntarily turn over their telephony metadata to Verizon, AT&T, and Sprint for various legitimate business purposes—in particular, to connect subscribers’ telephone calls. Then, like the third-party hospital in Ferguson, the phone companies have been transmitting this information to the government without subscribers’ consent or knowledge. While the program in Ferguson involved diagnostic test results and the NSA program deals with bulk telephony metadata, the programs are analytically the same. The NSA’s bulk collection of telephony metadata constitutes a “search” as it violates telephone subscribers’ reasonable expectation of privacy that their metadata will not be shared with non-telecommunications personnel. Of course, the government would contend that even if Ferguson limited the holding of Smith, it is simply not objectively reasonable for phone customers to have the same expectation of privacy in their metadata that prenatal hospital patients have in their

296. Ferguson, 532 U.S. at 82–85.
297. Id. at 70.
298. Id. at 70–73.
299. Id.
300. Id. at 76–78.
301. Id. at 95.
diagnostic test results. In the aftermath of the Snowden disclosures, the Obama Administration made precisely this argument—contending that the NSA program was not alarming or intrusive on the grounds “it’s just metadata” and that “[t]hey’re not looking at content.”

It is true that small amounts of telephony metadata might not be particularly revealing or personal, however, long-term metadata “reveal[s] more than the sum of its parts” and can be combined to form “a mosaic to reveal a full picture of a person’s life.” It is in this way that the logic of the concurring opinions in *Jones* complement *Ferguson*, and lead to the conclusion that the NSA’s bulk collection of telephony metadata constitutes a “search.” *Ferguson* teaches us that the Court is willing to extend Fourth Amendment protection to personal medical information voluntarily disclosed to a third-party hospital. In other words, the Court abrogated the per se rule of *Smith* that one can never have an objectively reasonable expectation of privacy in information voluntarily disclosed to a third party. And while we might not have a reasonable expectation of privacy in a small amount of telephony metadata compared to personal medical information, aggregate metadata collected over a long period of time is entirely different. The Supreme Court’s concurring opinions in *Jones* support this position—in the same way that an expectation of privacy in personal medical information can be reasonable, so can an expectation of privacy in long-term aggregate telephony metadata.

Former NSA General Counsel Stewart Baker has stated, “metadata absolutely tells you everything about somebody’s life. If you have enough metadata, you don’t really need content.” General Michael Hayden, former director of the NSA and the CIA later described Baker’s comments as totally correct and went further, asserting that “[w]e kill people based on metadata.” Computer security researcher, hacker, and core developer of the Tor project, Jacob Appelbaum, explains the immense power of metadata aggregated over time:

> So did anybody see on the subway [how you can] link your metro card to your debit card? . . . This is a concept, which is key to everything we’ll talk about today and its called “linkability.” . . . [I]f you have your metro card and you have your debit card—you have those things and you can draw a line between them . . . So that’s like, not a scary thing. Except your bankcard is maybe tied

---


306. Id.
to everything else that you do during the day. So now they know where you’re going, when you make purchases, and in theory, you should have some protections for these things. But the government has consistently said, that you actually have no protection and you have no assumption of privacy. So when they decide to target you, they can actually recreate your exact steps, with a metro card and with a credit card alone. Like literally where you go and what you buy and potentially by linking that data with other people on similar travel plans, they can figure out who you talked to and who you met with. When you then take cell phone data, which logs potentially your location . . . and you link up purchasing data, metro card data, and your debit card, you start to get what you could call metadata, in aggregate, over a person’s life. And metadata in aggregate is content.307

Numerous scholars, scientists, and journalists have echoed Appelbaum and Hayden’s comments regarding the extraordinary power of aggregate metadata.308 Mathematician Susan Landau, for example, has noted, “It’s much more intrusive than content. [The government can learn huge amounts of private information by studying] who you call, and who they call. If you can track that, you know exactly what is happening—you don’t need the content.”309 Metadata could reveal that someone called a suicide prevention hotline from the Brooklyn Bridge, but the topic of the phone call is secret.310 Likewise, it might reveal that “[someone] spoke with an HIV testing service, then [their] doctor, then [their] health insurance company in the same hour.”311 In sum, as Matt Blaze has explained in Wired Magazine, “Metadata is our context. And that can reveal far more about us . . . than the words we speak. Context yields insights into who we are and the implicit, hidden relationships between us.”312

Finally, Ferguson might be read as recognizing that the Court will grant Fourth Amendment protection in cases in which the government and a third party create a formalized policy under which a service provider collects information for law


310. Id.


312. Blaze, supra note 308.
enforcement officials. The Court has perhaps simply recognized that in such formalized circumstances, any information disclosed to a service provider ought to receive Fourth Amendment protection. If that is indeed the correct interpretation of Ferguson, the opinion is particularly relevant in Klayman and ACLU v. Clapper. In the same way that the hospital created a formalized program with law enforcement officials in Ferguson to turn over urine samples to the government for drug testing, Verizon, Sprint, and AT&T created a formalized program with the NSA to provide them with telephony metadata for all telephone calls made within United States on an ongoing and daily basis.

IV. CONCLUSION

It is debatable whether the NSA’s bulk collection of telephony metadata is or is not desirable public policy, but whether it constitutes a “search” under the Fourth Amendment will set precedent for an expanding horizon of technology including mass drone surveillance, cell phone tracking, and Internet metadata. While the NSA program might seem insignificant in that it tracks only telephony metadata without “content,” the possibility remains that technology will advance to the point where all information (visual, auditory, and olfactory) exposed in public could be collected, aggregated, and analyzed using complex algorithms over the lifetime of all American citizens. To be able to address this kind of aggregate and all-encompassing surveillance, the Court should follow its recent trend, relying particularly on a combination of Jones and Ferguson, to rule that the aggregate bulk collection of telephony metadata over time constitutes a “search” within the meaning of the Fourth Amendment.