Penn State Law Review

Volume 122 | Issue 3 Article 7

7-1-2018

Your Cooperation is Greatly Appreciated: The Fourth Amendment, National Security Letters and Public-Private Data Sharing

Kevin J. Schrop

Your Cooperation is Greatly Appreciated: The Fourth Amendment, National Security Letters, and Public-Private Data Sharing

Kevin J. Schrop*

ABSTRACT

In 2013, Edward Snowden leaked classified documents that revealed a massive surveillance program conducted by the National Security Agency (NSA). In revealing the NSA's surveillance program, the Snowden disclosures also detailed significant warrantless sharing of data between private U.S. communications companies and the U.S. government. Private communications companies collect and store the "metadata" of their customers in order to customize marketing and boost sales; however, these private companies often share this data with the government, who wants and uses this data for very different reasons.

While the Snowden disclosures created a public furor over the NSA's surveillance practices, the surveillance techniques of other U.S. agencies, in particular, the Federal Bureau of Investigation's (FBI) use of National Security Letters (NSLs), have garnered far less attention. Through NSLs, which are administrative subpoenas requiring no judicial oversight, the FBI can demand that private companies turn over the metadata they have collected on individuals. The FBI's power to issue NSLs is derived from two 1970s Supreme Court decisions concluding that an individual has no privacy right in information voluntarily given to a third party. This lack of an individual privacy right is known as the "third-party doctrine."

Although the Fourth Amendment of the U.S. Constitution protects Americans from illegal searches or seizures by the government, private entities are largely exempt from constitutional standards. However, the public-private data sharing revealed by Snowden raises questions regarding private companies' involvement in what would otherwise constitute Fourth Amendment violations. This Comment argues that the

* J.D. Candidate, The Pennsylvania State University School of Law, 2018. The author wishes to thank the *Penn State Law Review*, his mom and dad, the Calandriellos, and in particular, Fallon and Jack for their love and support.

transfer of personal data from private companies to the FBI under the authority of an NSL (1) allows the government to skirt the Fourth Amendment, (2) is unconstitutional, and (3) must end. The tenets of the third-party doctrine must be reconsidered in light of modern technology, and the entanglement exception embedded in constitutional jurisprudence provides an avenue through which the Fourth Amendment becomes applicable to private entities.

Table of Contents

I. INTRODUCTION

In June 2013, Edward Snowden, an employee of a private defense firm contracted by the National Security Agency (NSA), leaked top-secret documents that unveiled a massive surveillance program conducted by the NSA.[1] The initial disclosure revealed an order from the Foreign Intelligence Surveillance Court (FISC) that required the telecom giant Verizon to turn over millions of United States customers' telephone records to the NSA.[2] The FISC order required Verizon to turn over what is known as "metadata," which does not include the content of a communication, but instead includes information about the communication, such as the individuals involved in the communication, the time at which it took place, and its duration.[3] The Snowden disclosures led to "heighten[ed] public suspicion of the work of the intelligence agencies,"[4] and in response, many Americans took steps to "shield their information from the government"[5] or changed their use of technology.[6]

While the Snowden disclosures created a public outcry over the NSA's surveillance practices, the surveillance techniques of other U.S. agencies, and in particular the Federal Bureau of Investigation's (FBI) use of National Security Letters (NSLs), garnered far less attention.[7] Through the use of NSLs, which are administrative subpoenas requiring no judicial oversight, the FBI can demand that private companies turn over the metadata they have collected on individuals.[8] The FBI's power to issue NSLs is derived from two 1970s Supreme Court decisions,

1. *See* Glenn Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013, 9:00 AM), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

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

3. *See id.*

4. Alan Travis, *Snowden Leak: Governments' Hostile Reaction Fuelled Public's Distrust of Spies*, GUARDIAN (June 15, 2015, 11:19 AM), https://www.theguardian.com/world/2015/jun/15/snowden-files-us-uk-government-hostile-reaction-distrust-spies.

5. Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RES. CTR. (Mar. 16, 2015), www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.

6. *See id.* (finding that in the wake of the Snowden revelations, 17 percent of Americans changed their privacy settings on social media; 15 percent used social media less frequently; 15 percent avoided certain apps; 13 percent uninstalled apps; 14 percent spoke more frequently in person as opposed to online or on the phone; and 13 percent avoided using certain terms in online communications).

7. *See* Greenwald, *supra* note 2; Travis, *supra* note 4.

8. *See* 18 U.S.C. § 2709 (2012).

which concluded that an individual has no privacy right in information voluntarily given to a third party.[9] This lack of an individual privacy right is known as the third-party doctrine.[10]

The government relies on the third-party doctrine—through the use of NSLs—to acquire the data that corporations are constantly collecting on their customers.[11] While the government itself cannot conduct the kind of data collection and analysis that corporations engage in—because the Fourth Amendment of the U.S. Constitution protects Americans from illegal searches or seizures by the government—private entities are largely exempt from those constitutional standards, and thus, such data collection on their part is legal.[12] However, the public-private data sharing revealed by Snowden raises questions regarding private companies' involvement in what would otherwise constitute Fourth Amendment violations.[13] This Comment argues that the transfer of personal data from private companies to the FBI under the authority of an NSL (1) allows the government to skirt the Fourth Amendment, (2) is unconstitutional, and (3) must end.[14] The tenets of the third-party doctrine must be reconsidered in light of modern technology, and the entanglement exception embedded in constitutional jurisprudence provides an avenue through which the Fourth Amendment becomes applicable to private entities.[15]

This Comment will first provide a background of the Fourth Amendment and the evolution of the third-party doctrine.[16] Second, this Comment will discuss the state action requirement of the U.S. Constitution and the entanglement exception to the state action requirement.[17] Third, this Comment will discuss the history and current

9. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (concluding that individuals do not have a reasonable expectation of privacy in information conveyed by pen registers); United States v. Miller, 425 U.S. 435, 442–43 (1976) (concluding that an individual has no legitimate expectation of privacy in financial information voluntarily turned over to banks).

10. John Villasenor, *What You Need to Know About the Third-Party Doctrine*, ATLANTIC (Dec. 30, 2013), https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/.

11. *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 39 (2015).

12. *See* United States v. Stanley, 109 U.S. 3, 10, 17–18 (1883).

13. *See* Katz v. United States, 389 U.S. 347, 357 (1967) (stating that searches or seizures "conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions").

14. *See infra* Section III.C.

15. *See infra* Section III.C.

16. *See infra* Section II.A.

17. *See infra* Section II.B.

state of NSLs.[18] Fourth, this Comment will analyze recent Supreme Court and lower court decisions involving the third-party doctrine.[19] Finally, this Comment will analyze NSLs under the Fourth Amendment and offer recommendations for a possible path forward regarding the third-party doctrine.[20]

II. BACKGROUND

This Part will first discuss the Fourth Amendment and the jurisprudential evolution of the third-party doctrine.[21] Next, this Part will discuss the state action requirement of the U.S. Constitution and the entanglement exception to the state action requirement.[22] Finally, this Part will discuss the history and current state of NSLs.[23]

A. The Fourth Amendment and the Evolution of the Third-Party Doctrine

The Fourth Amendment protects citizens from unreasonable searches and seizures by the government.[24] As initially formulated, the Fourth Amendment protected citizens from searches or seizures of their "tangible material effects" or "actual physical invasion[s]" of their property.[25] However, the dawn of electronic communications changed this equation and required the United States Supreme Court to wrestle with a new and difficult question: How can 18th century privacy assumptions be squared with 20th century communications technology?[26]

The spread of electronic communications in the 20th century caused an increase in the by-products of electronic communications, which today is known as metadata.[27] With regards to electronic communications, metadata is non-content information about a communication, such as the numbers or accounts involved in a communication, when the communication took place, and how long the communication lasted.[28] In the 1970s, the Supreme Court developed the

18. *See infra* Section II.C.
19. *See infra* Sections III.A–.B.
20. *See infra* Section III.C.
21. *See infra* Section II.A.
22. *See infra* Section II.B.
23. *See infra* Section II.C.
24. U.S. CONST. amend. IV.
25. Olmstead v. United States, 277 U.S. 438, 466 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).
26. *See id.* at 464–66.
27. *See* SCHNEIER, *supra* note 11, at 15–20.
28. *See id.* at 24.

third-party doctrine,[29] creating a nominally constitutional avenue for the government to warrantlessly obtain the data individuals turn over to third parties in order to use their services.[30] Today, the third-party doctrine allows the government to warrantlessly acquire the mass amounts of metadata generated by Americans' use of electronic communications.[31]

This Section will first discuss the constitutional mandates of the Fourth Amendment and the Supreme Court's definitions of the terms "search" and "seizure."[32] This Section will then analyze the Court's first foray into electronic communications surveillance and the Fourth Amendment in *Olmstead v. United States*[33] in 1928.[34] Third, this Section will discuss the Court's famous 1967 *Katz v. United States*[35] decision, which provided the foundation for the third-party doctrine.[36] Finally, this Section will examine two cases from the 1970s, *United States v. Miller*[37] and *Smith v. Maryland*,[38] in which the Court articulated the third-party doctrine.[39]

1. The Fourth Amendment, its General Requirements, and the Definitions of "Search" and "Seizure"

The Fourth Amendment restricts certain investigatory and law enforcement powers of the government, providing that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[40]

The Fourth Amendment thus protects against unreasonable governmental intrusion by imposing three general requirements on a government search or seizure: (1) that it be reasonable; (2) that it be based on probable cause; and (3) that it be accomplished based on a warrant

29. *See* Smith v. Maryland, 442 U.S. 735, 741–42 (1979); *see also* United States v. Miller, 425 U.S. 435, 443 (1976).
30. *See* Villasenor, *supra* note 10.
31. *See id.*
32. *See infra* Section II.A.1.
33. Olmstead v. United States, 277 U.S. 438 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).
34. *See infra* Section II.A.2.a.
35. Katz v. United States, 389 U.S. 347 (1967).
36. *See infra* Section II.A.2.b.
37. United States v. Miller, 425 U.S. 435 (1976).
38. Smith v. Maryland, 442 U.S. 735 (1979).
39. *See infra* Section II.A.3.
40. U.S. CONST. amend. IV.

obtained through the judicial process.[41] In essence, Fourth Amendment jurisprudence balances an individual's privacy interests against the government's interests and the reasonableness of the government's conduct.[42]

The Supreme Court currently defines a "search" as an infringement on "an expectation of privacy that society is prepared to consider reasonable."[43] The Court in turn defines a "seizure" of property as a "meaningful interference with an individual's possessory interests in that property."[44] The Court has stated that searches or seizures "conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[45]

For most of American history, the terms "search" and "seizure" were not defined as broadly as they are now. Instead, the terms were limited to the search or seizure of a person's "tangible material effects" or an "actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."[46] These limitations were sensible in an era when a person's "papers" and "effects" were all "tangible" and where some sort of "actual physical invasion" was required to execute a search or seizure.[47] However, in a world where communications and information are often intangible and where communications and information can be searched or seized without an "actual physical invasion," these definitions become anachronistic and ineffectual.[48]

41. *See* Theodore P. Metzler et al., *Warrantless Searches and Seizures*, 89 GEO. L.J. 1084, 1084 (2001). However, the Supreme Court has recognized several exceptions to these requirements. While the exceptions to the Fourth Amendment's warrant and probable cause requirements are largely outside the scope of this Comment and will not be discussed here, they include: investigatory detentions; warrantless arrests; searches incident to arrest; plain view; exigent circumstances; consent searches; vehicle searches; container searches; inventory searches; border searches; searches at sea; administrative searches; and special needs searches. *Id.*

42. *See* United States v. Jacobsen, 466 U.S. 109, 125 (1984).

43. *Id.* at 113.

44. *Id.*

45. Katz v. United States, 389 U.S. 347, 357 (1967) (emphasis in original) (footnote omitted) (referring to "searches" under the Fourth Amendment, although the same general sentiment pertains to "seizures," as the Court makes evident in the text preceding the language quoted here); *accord* Metzler et al., *supra* note 41, at 1084.

46. Olmstead v. United States, 277 U.S. 438, 466 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

47. *Id.*

48. *Id.*

2. Electronic Surveillance and the Fourth Amendment

Based on these changes in communications and, in particular, the advent of electronic communications, the Supreme Court reexamined its Fourth Amendment jurisprudence.[49] Although the Court initially refused to adapt its Fourth Amendment analysis to electronic communications,[50] by the late 1960s the Court developed the test that has guided Fourth Amendment jurisprudence to the present day: the *Katz* test.[51]

a. The *Olmstead* Definition of Search and Seizure

The Supreme Court first dealt with the novel constitutional issues posed by electronic communications and surveillance in its 1928 decision in *Olmstead*.[52] In *Olmstead*, the Court decided whether evidence of private telephone conversations obtained via wiretap, without a warrant, violated the Fourth Amendment.[53] In upholding the petitioners' conviction for conspiracy to violate the National Prohibition Act,[54] the Court concluded that wiretapping "did not amount to a search or seizure within the meaning of the Fourth Amendment" and therefore did not require a warrant.[55]

The Court in *Olmstead* reasoned that although Congress could take action to "protect the secrecy of telephone messages," the Court could not approve of such an "enlarged and unusual" interpretation of the Fourth Amendment as the petitioners had suggested.[56] The Court stated that the "reasonable" view of warrantless wiretapping is that a person who installs a telephone in his or her home "intends to project his voice to those quite outside," and that the Fourth Amendment does not protect "the wires beyond his house and messages while passing over them."[57] The Court concluded that absent an "official search . . . of his person, . . . his papers or his tangible material effects[,] or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure," there was no violation of the Fourth Amendment.[58]

---

49. *See id.* at 464–65.

50. *See id.* at 465–66 ("Congress may, of course, protect the secrecy of telephone messages . . . [b]ut the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the Fourth Amendment.").

51. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

52. *See Olmstead*, 277 U.S. at 464–66.

53. *See id.* at 455.

54. National Prohibition Act, ch. 85, 41 Stat. 305 (1919), *repealed by* U.S. CONST. amend. XXI.

55. *Olmstead*, 277 U.S. at 466.

56. *Id.* at 465–66.

57. *Id.* at 466.

58. *Id.*

b. A New View of the Fourth Amendment in *Katz*

For nearly 40 years, the *Olmstead* decision stood as the Court's view of the relationship between electronic communications, surveillance, and the Fourth Amendment.[59] However, in 1967, the Court again took up the issue of the warrantless wiretapping of electronic communications in its momentous *Katz* decision.[60] In *Katz*, the Court not only partially overturned *Olmstead* and established the course of the Court's modern Fourth Amendment surveillance jurisprudence, but also laid the foundation for what would become known as the third-party doctrine.[61]

In *Katz*, the Court examined whether the FBI violated the petitioner's Fourth Amendment rights when, without a warrant, FBI agents placed a listening device on the outside of a public phone booth that the petitioner used to place illegal bets.[62] The Court rejected the government and lower court's reasoning that there could be no Fourth Amendment violation without a "physical entrance"[63] by the government,[64] and went on to dismiss as irrelevant an argument regarding whether a public phone booth was a constitutionally protected zone.[65] The Court stated that the "Fourth Amendment protects people, not places,"[66] and that it was unimportant that the recording device did not breach the phone booth.[67] The Court determined that the FBI's actions "violated the privacy upon which [the petitioner] justifiably relied," and were a "'search or seizure' within the meaning of the Fourth Amendment."[68]

The Court in *Katz* reasoned—significantly for the future third-party doctrine—that what one "knowingly exposes to the public" is not protected by the Fourth Amendment,[69] but what one "seeks to preserve as private," even in public, may deserve constitutional protection.[70] The

59. *See* Tom McInnis, *The Changing Definition of Search or Seizure*, 11 INSIGHTS ON L. & SOC'Y 10, 11 (2011).
60. *See generally* Katz v. United States, 389 U.S. 347 (1967).
61. *See id.* at 351 (citing Lewis v. United States, 385 U.S. 206, 210 (1966); United States v. Lee, 274 U.S. 559, 563 (1927)).
62. *Id.* at 348–50.
63. *Id.* at 349 (quoting Katz v. United States, 369 F.2d 130, 134 (9th Cir. 1966)).
64. *Id.* at 352–53.
65. *See id.* at 351.
66. *Id.*
67. *See id.* at 353.
68. *Id.*
69. *Id.* at 351 (citing Lewis v. United States, 385 U.S. 206, 210 (1966); United States v. Lee, 274 U.S. 559, 563 (1927)).
70. *Katz*, 389 U.S. at 351 (citing Rios v. United States, 364 U.S. 253 (1960); *Ex parte* Jackson, 96 U.S. 727, 733 (1877)).

Court concluded that the evidence the FBI obtained through the listening device should be excluded, despite the limited nature of the agents' actions and their reliance on earlier judicial precedent, because the FBI had acted without prior judicial approval.[71] The Court stated that although the agents' actions would have received judicial sanction, "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment."[72]

The *Katz* decision laid the foundation for the Court's modern Fourth Amendment surveillance jurisprudence and updated the Court's definitions of search and seizure.[73] Interestingly, the most influential feature of the *Katz* decision was not the opinion itself, but was Justice Harlan's concurring opinion that formulated the "expectation of privacy" test for future jurisprudence.[74] Justice Harlan stated that the Fourth Amendment protects an individual that has an "actual (subjective) expectation of privacy," and an "expectation . . . that society is prepared to recognize as 'reasonable.'"[75] Justice Harlan's two-pronged conception, consisting of subjective and objective elements, proved crucial for future Fourth Amendment jurisprudence and became the foundation of the third-party doctrine.[76]

3. The Birth of the Third-Party Doctrine: *Miller* & *Smith*

The third-party doctrine, established by the Supreme Court's 1976 decision in *Miller*, states that an individual has no legitimate expectation of privacy in "information revealed to a third party."[77] In *Miller*, the Court examined whether the production of documents by the respondent's bank in response to a subpoena violated the respondent's Fourth Amendment interest.[78] The Court stated that the respondent "possessed no Fourth Amendment interest" in the subpoenaed documents,[79] and reasoned that a "depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the [g]overnment."[80] Further, the Court stated that even if the information is offered to the third party in the expectation that it will be

71. *See id.* at 356.
72. *Id.* at 357 (emphasis in original) (footnote omitted).
73. *See id.* at 350–54.
74. *See id.* at 361 (Harlan, J., concurring).
75. *Id.*
76. *See* United States v. Miller, 425 U.S. 435, 442–43 (1976).
77. *Id.* at 443.
78. *Id.* at 436–37.
79. *Id.* at 445.
80. *Id.* at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971)).

"used only for a limited purpose," the Fourth Amendment is still not violated when that information is subsequently turned over to the government.[81] The Court in *Miller* applied the *Katz* test enunciated by Justice Harlan and concluded that when an individual reveals information to a third party, he or she may have a subjective, but never an objective, expectation of privacy.[82]

Three years later in the Court's decision in *Smith*, the Supreme Court extended its ruling in *Miller* and strengthened the third-party doctrine.[83] In *Smith*, the Court concluded that the non-content data generated by phone calls and collected by a pen register at a telephone company's office came under the third-party doctrine, and, thus, was not protected by the Fourth Amendment.[84] In reaching its decision, the Court noted the "limited capabilities" of pen registers and the fact that they did not gather the "*contents* of communications"; in other words, pen registers only collected an early form of metadata.[85] The Court in *Smith* then explicitly relied on *Katz* and *Miller* and stated that the petitioner had voluntarily conveyed the non-content data to a third party, so he likely had not had an "actual expectation of privacy" and certainly had not had an expectation of privacy society found "legitimate."[86]

The Court developed the third-party doctrine based on the *Katz* test, as formulated by Justice Harlan, and delineated its meaning in *Miller* and *Smith*.[87] Although the *Katz* test seemed to strengthen individuals' privacy rights by broadening the Fourth Amendment's applicability beyond the Amendment's specific textual provisions,[88] the third-party doctrine that emerged from the *Katz* test seemed to do the opposite, and potentially

81. *Id.*

82. *See id.* at 442–43 (stating that the Fourth Amendment is not violated "even if 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" because there is no "legitimate expectation of privacy concerning information kept in bank records").

83. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979).

84. *See id.* at 744–46.

85. *Id.* at 741–42 (emphasis added). Discussing the capabilities of pen registers, the Court stated: "[Pen registers] disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." *Id.* (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)).

86. *Id.* at 745.

87. *See id.* at 744; *Miller*, 425 U.S. at 443; Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

88. *Katz*, 389 U.S. at 352–53 (noting that while "[i]t is true that the absence of such [physical] penetration was at one time thought to foreclose further Fourth Amendment inquiry, for the Amendment was thought to limit only searches and seizures of tangible property," the Court no longer holds that "narrow view").

made the "most intimate details of a person's life" more vulnerable.[89] This danger is especially clear in the age of the Internet, where almost all of one's communications, finances, and personal information are online and stored with private third parties that do not necessarily have to comply with the mandates of the Constitution due to the state action requirement.[90]

B. The State Action Requirement and Its Exceptions

While the government must adhere to the provisions of the Constitution and the Bill of Rights, private parties and individuals are generally not required to so adhere,[91] although there are exceptions to this rule.[92] The Supreme Court has recognized that in certain circumstances, private parties are so closely involved with the government[93] or are performing functions traditionally fulfilled exclusively by the government[94] that they become the government for constitutional purposes.[95] In these situations, private entities come under the Constitution's purview and must comply with constitutional commands.[96]

1. The State Action Requirement

The United States Constitution and the Bill of Rights originally applied only to the federal government, meaning that their limitations and protections did not apply to the acts or actions of states, private entities, or individuals.[97] However, after the Civil War, the states ratified the Fourteenth Amendment, and for the first time an amendment to the

89. *See Smith*, 442 U.S. at 748 (Stewart, J., dissenting).

90. *See* SCHNEIER, *supra* note 11, at 80.

91. *See* U.S. CONST. amend. XIV; *see also* United States v. Stanley, 109 U.S. 3, 10–11, 17–18 (1883).

92. *See* Erwin Chemerinsky & Martin A. Schwartz, *Dialogue on State Action*, 16 TOURO L. REV. 775, 780–90 (2016).

93. *See* Shelley v. Kraemer, 334 U.S. 1, 18–19 (1948) (concluding that judicial enforcement of discriminatory private agreements by state courts qualifies as state action).

94. *See generally* Jackson v. Metro. Edison Co., 419 U.S. 345, 352 (1974) (noting that the Court has found state action where a private entity exercises powers that are traditionally only exercised by the State); Terry v. Adams, 345 U.S. 461, 483–84 (1953) (concluding that a private political club which "operate[d] as an auxiliary of the local Democratic Party" acquired the attributes of the government and must be treated like the State for constitutional purposes).

95. *See* Chemerinsky & Schwartz, *supra* note 92, at 780–90.

96. *See id.*

97. *See* Barron v. Mayor and City Council of Balt., 32 U.S. 243, 250–51 (1833) (concluding that the Bill of Rights were not intended to apply to the states and only limit the actions of the federal government).

Constitution prohibited particular categories of state action.[98] Congress then passed the Civil Rights Act[99] in 1875, which required equal access to certain public accommodations for all citizens, regardless of color or previous condition of servitude, and penalized any individual who did not comply.[100] In *United States v. Stanley*,[101] the Court, in deciding whether the Fourteenth Amendment gave Congress the power to enact the Civil Rights Act, first articulated the state action requirement.[102]

In *Stanley*, the Court examined the Fourteenth Amendment and noted that it prohibited "State action of a particular character" and not the "[i]ndividual invasion of individual rights."[103] The Court continued by stating that absent a state law or state agents' or officers' actions contrary to the rights of a citizen, "no legislation of the United States under said [Fourteenth] amendment, nor any proceeding under such legislation, can be called into activity."[104] The Court concluded that parts of the Civil Rights Act were therefore unconstitutional because they prohibited and penalized actions of private individuals, whereas the Fourteenth Amendment only prohibited certain actions by states.[105] Reasoning that civil rights "cannot be impaired by the wrongful acts of individuals, unsupported by State authority in the shape of laws, customs, or judicial or executive proceedings,"[106] the Court ultimately pronounced the state action requirement.[107]

2. Exceptions to the State Action Requirement

The state action requirement generally means that private conduct does not need to comply with the Constitution.[108] While Congress and state legislatures can apply constitutional norms to private conduct through legislation, an action brought under these statutes does not indicate a constitutional violation or emanate from a constitutional right.[109] However, the Court has recognized two main exceptions to the

98. U.S. CONST. amend. XIV; *see* United States v. Stanley, 109 U.S. 3, 13 (1883).
99. Civil Rights Act of 1875, ch. 114, 18 Stat. 335, *invalidated* by *Stanley*, 109 U.S. at 11.
100. *See id.* §§ 1–2, 18 Stat. at 336.
101. United States v. Stanley, 109 U.S. 3 (1883).
102. *See id.* at 10–11, 13.
103. *Id.* at 11.
104. *Id.* at 13.
105. *See id.* at 11, 22, 26.
106. *Id.* at 17.
107. *See id.* at 11, 17–18.
108. *See id.* at 17–18.
109. ERWIN CHEMERINSKY, CONSTITUTIONAL LAW 548 (4th ed. 2013).

state action requirement, the most important for purposes of this Comment being the entanglement exception.[110]

The entanglement exception states that state action exists where the government "affirmatively authorizes, encourages, or facilitates unconstitutional action."[111] The Court articulated the entanglement exception to the state action requirement in the 1948 case of *Shelley v. Kraemer*.[112] In *Shelley*, the Court—after consolidating two separate cases—had to decide whether state court enforcement of restrictive covenants implicated the state sufficiently to qualify as a state action, and if so, whether that action denied the petitioners equal protection.[113] The Court stated that the cases undoubtedly involved state action[114] and determined that in "granting judicial enforcement of these restrictive agreements," the petitioners were denied equal protection.[115]

The Court reasoned that the state courts involved in the enforcement of restrictive covenants had not "merely abstained from action" and allowed private discrimination to occur, but rather had provided to those attempting to enforce the covenants "the full coercive power of government."[116] Further, the state courts not only made the government's coercive power available to these individuals, but they also were the cause-in-fact of the equal protection violation.[117] As the Court stated, "but for the active intervention of the state courts," the restrictive covenants would have been unenforceable.[118] In sum, the judicial enforcement of discriminatory private covenants sufficiently involved the state in private discrimination so as to be considered an action of the state.[119]

The entanglement exception to the state action requirement broadened the reach of the Constitution and required private entities sufficiently involved with the government to adhere to constitutional norms.[120] However, this rather straightforward idea becomes more

110. *See* Chemerinsky & Schwartz, *supra* note 92, at 780–86. The second exception referred to above, the public functions exception, is beyond the scope of this Comment and will not be discussed further. For discussions of the public functions exception, see Jackson v. Metro. Edison Co., 419 U.S. 345, 352–53 (1974); Evans v. Newton, 382 U.S. 296, 302 (1966); Terry v. Adams, 345 U.S. 461, 468–70 (1953); and Marsh v. Alabama, 326 U.S. 501, 506 (1946).

111. Chemerinsky & Schwartz, *supra* note 92, at 780.

112. Shelley v. Kraemer, 334 U.S. 1, 18–19 (1948).

113. *See id.* at 18.

114. *Id.* at 19.

115. *Id.* at 20.

116. *Id.* at 19.

117. *See id.*

118. *Id.*

119. *See id.* at 19–20.

120. *See* Chemerinsky & Schwartz, *supra* note 92, at 780.

complicated when modern communications technology, national security, and a competing constitutional doctrine are injected into the equation. While the entanglement exception requires certain private parties to comply with the Constitution, the third-party doctrine pulls in the other direction and seemingly allows the government to skirt constitutional mandates.[121] Further, the third-party doctrine provides the legal foundation for a key national security tool of the FBI: National Security Letters.[122]

C. *Accessing Third-Party Records: The FBI and National Security Letters*

National Security Letters (NSLs) are administrative subpoenas issued by the FBI to certain custodians of third-party records in terrorism and espionage cases.[123] The FBI employs five types of NSLs,[124] though this Comment will only focus on Electronic Communications Privacy Act[125] (ECPA) NSLs issued pursuant to 18 U.S.C. § 2709.[126] The FBI uses NSLs under § 2709 to obtain subscriber information and toll billing and transactional records from electronic communication service providers (CSPs).[127] While the FBI can obtain metadata from CSPs, it cannot acquire the content of communications under § 2709.[128] Since the turn of the century, the FBI has issued over 300,000 NSLs.[129]

---

121. *Compare Shelley*, 334 U.S. at 18–20, *with* Smith v. Maryland, 442 U.S. 735, 744–46 (1979), *and* United States v. Miller, 425 U.S. 435, 443 (1976).

122. *See infra* Section II.C.

123. Michael German et al., *National Security Letters: Building Blocks for Investigations or Intrusive Tools?*, ABA J. (Sept. 1, 2012), www.abajournal.com/magazine/article/national_security_letters_building_blocks_for_investigations_or_intrusive_t/.

124. *See id.* (listing and discussing the history of the five different acts under which NSLs are issued: the Electronic Communications Privacy Act; the Right to Financial Privacy Act; the Fair Credit Reporting Act; the National Security Act; and the USA PATRIOT Act).

125. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

126. 18 U.S.C. § 2709 (2012).

127. *Id.* § 2709(a); *see also id.* § 2510 (defining "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications"). Although the statute does not define "electronic communication service provider," the definition can be inferred from the definition of "electronic communications service" and includes companies like Yahoo, Google, or Verizon.

128. *See* German et al., *supra* note 123; *see also National Security Letters*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/nsl/ (last visited Nov. 21, 2016).

129. Kim Zetter, *Yahoo Publishes National Security Letters After FBI Drops Gag Orders*, WIRED (June 1, 2016, 4:41 PM), https://www.wired.com/2016/06/yahoo-publishes-national-security-letters-fbi-drops-gag-orders/.

In 1986, Congress passed the ECPA in an effort to reform existing wiretapping and electronic surveillance laws.[130] After the terrorist attacks of September 11, 2001, Congress passed the USA PATRIOT Act[131] and expanded the reach of the ECPA and NSLs.[132] In 2006, Congress again amended the ECPA,[133] and in 2015, in response to the Snowden disclosures, Congress passed the USA FREEDOM Act,[134] which reformed the ECPA and the function of NSLs.[135]

1. The Electronic Communications Privacy Act of 1986

Congress first authorized the use of NSLs in the ECPA of 1986.[136] In Section 201 of the ECPA, Congress granted the FBI the power to order a third-party CSP to turn over certain customer information or records upon request by the Director of the FBI or his designee.[137] Section 201 stipulated that the request must be in writing and must be relevant to a legal foreign counterintelligence investigation of a foreign power or its agent(s) whose identity must be based on "specific and articulable facts."[138] Section 201 also prohibited a CSP from disclosing the receipt of an NSL, permitted the FBI to disseminate the information subject to certain guidelines, and required the FBI to update certain congressional bodies twice a year.[139] Despite Section 201's strong language, the enforcement and legal penalties for noncompliance with an FBI request or for disclosing such a request were unclear, though Congress would soon clarify these matters.[140]

---

130. *See Electronic Communications Privacy Act (ECPA)*, ELECTRONIC PRIVACY INFO. CTR., https://www.epic.org/privacy/ecpa/ (last visited Jan. 19, 2017).

131. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

132. *See* CHARLES DOYLE, CONG. RESEARCH SERV., RS22406, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE AT THE LEGAL BACKGROUND 3–4 (2015).

133. *See id.* at 5.

134. Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

135. *See id.* §§ 501–503, 129 Stat at 282–91.

136. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1867–68 (codified as amended at 18 U.S.C. § 2709 (2012)).

137. *Id.* § 201, 100 Stat. at 1867 (codified as amended at 18 U.S.C. § 2709(a)) (stating that communication service providers have a "[d]uty to [p]rovide . . . subscriber information and toll billing records information, or electronic communication transactional records").

138. *Id.* (codified as amended at 18 U.S.C. § 2709(b)).

139. *Id.* § 201, 100 Stat. at 1867–68 (codified as amended at 18 U.S.C. § 2709(c)–(e)).

140. *See* CHARLES DOYLE, CONG. RESEARCH SERV., RS22406, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE AT THE LEGAL BACKGROUND 2 (2015).

2. USA PATRIOT Act of 2001

In the wake of the terrorist attacks of September 11, 2001, Congress passed the USA PATRIOT Act and expanded the scope of ECPA NSLs.[141] The USA PATRIOT Act amended the ECPA in five key ways: (1) it granted the heads of FBI field offices the power to issue NSLs, instead of restricting this authority solely to officials at FBI headquarters; (2) it removed the requirement that NSLs be related to a foreign power or its agents; (3) it removed the "specific and articulable facts" requirement for believing that the subject of the NSL was a foreign power or an agent of such; (4) it altered the requirement that NSLs be related to a foreign counterintelligence investigation and instead only required that NSLs be related to combating international terrorism or foreign espionage; and (5) it protected Americans against investigation solely based on First Amendment activities.[142] Through the USA PATRIOT Act amendments to the ECPA, Congress authorized the FBI to employ its NSL authority both more rapidly and expansively.[143]

3. 2006 PATRIOT Act Reauthorization Amendments

In 2006, Congress reauthorized and significantly amended 18 U.S.C. § 2709, adding provisions regarding the judicial review and enforcement of NSLs and nondisclosure requirements.[144] One significant amendment permitted a CSP to seek judicial review of an NSL and to have the request altered or vacated if it was "unreasonable, oppressive, or otherwise unlawful."[145] Congress also provided for judicial review of NSL nondisclosure requirements, though a court would only be required to modify or vacate the requirement if there was no evidence that such disclosure would threaten national security, ongoing investigations, diplomatic relations, or an individual's safety.[146]

---

141. *See id.* at 3–4.

142. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 505, 115 Stat. 272, 365–66 (codified as amended at 18 U.S.C. § 2709(b)); *see also* CHARLES DOYLE, CONG. RESEARCH SERV., RS22406, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE AT THE LEGAL BACKGROUND 3 (2015).

143. CHARLES DOYLE, CONG. RESEARCH SERV., RS22406, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE AT THE LEGAL BACKGROUND 4 (2015).

144. *See id.* at 5.

145. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-77, § 115, 120 Stat. 192, 211–13 (2006) (codified as amended at 18 U.S.C. § 3511).

146. *Id.* § 115, 120 Stat. at 211–12. This provision explained:

> [T]he court may modify or set aside such a nondisclosure requirement if . . . there is no reason to believe that disclosure may endanger the national security

In providing for judicial review of NSL nondisclosure requirements, Congress also created guidelines for such judicial review that were highly deferential to the government.[147] Congress further provided for judicial enforcement of NSLs[148] and gave restrictive parameters under which a CSP could disclose receipt of an NSL.[149] Through the 2006 amendments to § 2709, Congress created a process by which a CSP could challenge an NSL and/or its nondisclosure requirement, albeit in a process that still weighed heavily in favor of the government.[150]

4. USA FREEDOM Act of 2015

After learning about the scope of NSA surveillance via the Snowden disclosures of 2013, the American public became increasingly suspicious of government surveillance.[151] Later that year, in response to the public's reaction to the Snowden disclosures, President Obama established a Review Group on Intelligence and Communications Technology ("Review Group").[152] The Review Group offered numerous recommendations, many of which dealt with NSLs, including requiring that NSLs be judicially approved and increasing the oversight and transparency of the NSL process.[153]

In June 2015, Congress offered its own response to the Snowden disclosures by passing the USA FREEDOM Act ("Act"), which ended the NSA bulk collection program.[154] Although Congress did not adopt

---

> of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life . . . of any person.

Id.

147. *See id.* (providing that certification by specified officials that disclosure would threaten national security, an ongoing investigation, diplomatic relations, or the safety of an individual would be "treated as conclusive unless the court finds that certification was made in bad faith").

148. *Id.* § 115, 120 Stat. at 212–13 (granting district courts the power to "compel compliance" with an NSL).

149. *See id.* § 116, 120 Stat. at 213 (codified as amended at 18 U.S.C. § 2709(c)) (permitting the recipient of an NSL to disclose such receipt to "persons necessary to comply with the request" or to counsel "to obtain legal advice or legal assistance with respect to the request" as long as the individuals to whom the NSL is disclosed are informed of the nondisclosure requirement).

150. *See generally id.* §§ 115–116, 120 Stat. at 211–17.

151. *See* Travis, *supra* note 4.

152. *See* CHARLES DOYLE, CONG. RESEARCH SERV., RS22406, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE AT THE LEGAL BACKGROUND 14 (2015).

153. *See id.* (noting three recommendations of the Review Group related to NSLs: (1) judicial approval of NSLs except in emergencies; (2) subjecting NSLs to Section 215 minimization requirements; and (3) greater oversight and public transparency for NSLs).

154. *See* Kim Zetter, *The Senate Finally Passes NSA Surveillance Reform*, WIRED (June 2, 2015, 4:42 PM), https://www.wired.com/2015/06/senate-finally-passes-bit-nsa-

the specific policy recommendations of President Obama's Review Group in the Act,[155] the legislation did amend § 2709 in several ways similar to the Review Group's policy recommendations.[156] Specifically, the Act prohibited the bulk collection of telephone toll and transactional records,[157] reformed the nondisclosure requirement procedures,[158] and required the Attorney General to create termination procedures for nondisclosure requirements.[159] Further, the Act altered the process of judicial review of nondisclosure requirements[160] and mandated that the Director of National Intelligence publish an annual report on the Internet regarding the government's use of NSLs.[161] Finally, the Act permitted a party subject to a nondisclosure requirement under an NSL to publish a report stating the number of NSLs the party received and the number of customers affected by such requests.[162] However, the Act required the

reform/ (noting that while the USA FREEDOM Act ended the NSA's bulk collection and storage of phone records, telecom companies were still collecting and storing this information and the government could access it by court order).

155. *See* CHARLES DOYLE, CONG. RESEARCH SERV., RS22406, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE AT THE LEGAL BACKGROUND 17 (2015).

156. *See generally* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Public L. No. 114-23, §§ 501–503, 129 Stat. 268, 282–91 (codified at 18 U.S.C. § 2709 (2012)).

157. *Id.* § 501, 129 Stat. at 282 (amending the existing statute by requiring a request under 18 U.S.C. § 2709(b) to include a "term that specifically identifies a person, entity, telephone number, or account as the basis of a request").

158. *Id.* § 502, 129 Stat. at 283 (amending the existing statute by basing enforceability of a nondisclosure agreement on two facts: (1) the recipient of an NSL must be notified of the right to judicial review; and (2) the order must include certification by an appropriate official that disclosure could threaten national security, an ongoing investigation, diplomatic relations, or an individual's safety).

159. *Id.* § 502, 129 Stat. at 288 (requiring within 180 days that the Attorney General establish guidelines to: (1) review and assess whether facts exist to continue a nondisclosure requirement; (2) terminate nondisclosure requirements no longer supported by existing facts; and (3) provide notice to NSL recipients that a nondisclosure requirement has been terminated).

160. *Id.* § 502, 129 Stat. at 288–89 (allowing judicial review of nondisclosure requirement to be commenced by a recipient petitioning the government or a court; requiring that within 30 days of receiving notice of a challenge to a nondisclosure requirement the government must apply for continuing nondisclosure based on "a statement of specific facts" showing the need for the nondisclosure requirement; and providing that the judicial standard of review of nondisclosure agreements is whether there is "reason to believe" nondisclosure is necessary to protect national security, an ongoing investigation, diplomatic relations, or an individual's safety).

161. *Id.* § 602, 129 Stat. at 292–93 (requiring the Director of National Intelligence to publish the "total number of national security letters issued and the number of requests for information contained within such national security letters").

162. *Id.* § 603, 129 Stat. at 295–96; *see also* CHARLES DOYLE, CONG. RESEARCH SERV., RS22406, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE AT THE LEGAL BACKGROUND 19 (2015).

reports to be published in a pre-approved format that presented the relevant figures in broad ranges.[163]

5. 18 U.S.C. § 2709 Today

Section 2709 presently grants the FBI broad authority to coerce CSPs into producing customer metadata.[164] The FBI may compel, upon specifically identifying a "person, entity, telephone number, or account," a CSP to turn over to the FBI customer information, billing records, and transactional data in the CSP's possession.[165] Section 2709(c)(1) also maintains the nondisclosure requirement on CSPs, provided that the FBI certifies that a CSP disclosure of the receipt of an NSL may cause danger to national security or an individual or may interfere with an investigation or diplomatic relation.[166] Finally, § 2709 provides exceptions to the prohibition on disclosure,[167] allows for judicial review of NSL requests and the nondisclosure requirements,[168] requires the FBI Director to provide updates to certain congressional committees twice a year,[169] and permits the FBI to disseminate the information it gathers pursuant to an NSL in some circumstances.[170]

---

163. § 604, 129 Stat. at 295–96; *see also* CHARLES DOYLE, CONG. RESEARCH SERV., RS22406, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE AT THE LEGAL BACKGROUND 19(2015).

164. *See generally* 18 U.S.C. § 2709 (2012).

165. *Id.* § 2709(a)–(b) (stating that the FBI "may, using a term that specifically identifies a person, entity, telephone number, or account as the basis for a request—(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity" as long as it is certified in writing that this information is relevant to "protect against international terrorism or clandestine intelligence activities" and is not conducted against a United States person "solely on the basis of activities protected by the first amendment").

166. *Id.* § 2709(c)(1) (prohibiting disclosure of a receipt of an NSL by CSPs or an "officer, employee, or agent thereof" when it is certified that the "absence of a prohibition of disclosure . . . may result in—(i) a danger to the national security of the United States; (ii) interference with a criminal, counterterrorism, or counterintelligence investigation; (iii) interference with diplomatic relations; or (iv) danger to the life or physical safety of any person").

167. *Id.* § 2709(c)(2)(A) (permitting the recipient of an NSL to disclose that fact to "(i) those persons to whom disclosure is necessary in order to comply with the request"; (ii) an attorney; or (iii) "other persons" specified by the FBI).

168. *Id.* § 2709(d) (permitting judicial review of a request or nondisclosure requirement pursuant to 18 U.S.C. § 3511).

169. *Id.* § 2709(f) (requiring the Director of the FBI to "fully inform the Permanent Select Committee on Intelligence of the House . . . and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House . . . and the Committee on the Judiciary of the Senate, concerning" certain requests made twice a year).

170. *Id.* § 2709(e). This provision permits the FBI to:

> [D]isseminate information . . . obtained . . . only as provided in guidelines approved by the Attorney General for foreign intelligence . . . and foreign

In the ECPA of 1986, Congress gave the FBI the power to issue NSLs to CSPs, an authority grounded in the third-party doctrine and one that Congress has modified and strengthened several times since.[171] The next Part of this Comment will discuss two recent Supreme Court cases that called into question certain tenets of the third-party doctrine,[172] and how lower courts have interpreted metadata and the third-party doctrine.[173] Finally, this Comment will examine why the Fourth Amendment applies to the FBI's use of NSLs and why, absent the third-party doctrine, the FBI's use of NSLs is unconstitutional, and, ultimately, will argue that the Supreme Court should do away with the third-party doctrine.[174]

III. ANALYSIS

The Supreme Court should reevaluate the third-party doctrine in light of 21st century technology and a recent Supreme Court decision.[175] The growth of corporate surveillance,[176] coupled with the vast amounts of metadata that individuals involuntarily generate and transfer to third parties in everyday activities,[177] has made obtaining the content of communications unnecessary for effective surveillance.[178] In short, without the judicially created third-party doctrine, § 2709 and NSLs would likely be deemed unconstitutional because they coerce private parties into participating in warrantless searches by the federal government.[179]

This Part will begin by examining two recent Supreme Court decisions that question the underpinnings of the third-party doctrine and

---

> counterintelligence investigations conducted by the [FBI], and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the . . . responsibilities of such agency.

Id.

171. *See supra* Section II.C.

172. *See infra* Section III.A.

173. *See infra* Section III.B.

174. *See infra* Section III.C.

175. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

176. *See* SCHNEIER, *supra* note 11, at 27–28.

177. *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

178. *See* SCHNEIER, *supra* note 11, at 27. Schneier quotes a former NSA general counsel who stated as follows: "Metadata absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content." *Id.*

179. *See* Katz v. United States, 389 U.S. 347, 357 (emphasis added) (footnote omitted) (stating that searches "conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions").

thus raise doubts about the constitutionality of § 2709 and NSLs.[180] Next, this Part will briefly discuss how lower courts have applied the third-party doctrine in light of 21st century electronic communications metadata.[181] Finally, this Part will close by discussing why the Fourth Amendment applies to the FBI's use of NSLs, and why, in the absence of the judicially created third-party doctrine, this practice violates the Fourth Amendment and is unconstitutional.[182]

A. The Third-Party Doctrine in the Twenty-First Century: A New View for the Supreme Court?

Although the Supreme Court has never directly ruled on the constitutionality of § 2709 or NSLs,[183] some of the Court's more recent decisions suggest that the third-party doctrine, and thus § 2709, could be on shaky ground.[184] While this assessment hinges to some degree on the ideological makeup of the Court, both the Court and individual Justices have made statements that undermine the legal foundations of § 2709.[185]

1. The Dynamic Nature of Privacy Expectations: *City of Ontario v. Quon*

The Supreme Court scratched the outer edges of the third-party doctrine in the 2010 case of *City of Ontario v. Quon*.[186] In *Quon*, the Court was faced with the issue of whether the respondent's employer, the City of Ontario Police Department, violated the respondent's Fourth Amendment rights when it read transcripts of text messages he sent and received from a work-issued pager.[187] The Court concluded that the city's review of the transcripts was reasonable and did not violate the Fourth Amendment because it was "not 'excessively intrusive'" and was

180. *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring); City of Ontario v. Quon, 560 U.S. 746, 759 (2010); *infra* Section III.A.

181. *See, e.g.*, United States v. Carpenter, 819 F.3d 880, 886 (6th Cir. 2016), *cert granted*, 137 S. Ct. 2211 (2017); *infra* Section III.B.

182. *See infra* Section III.C.

183. *See National Security Letters*, *supra* note 128.

184. *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."); *see also Quon*, 560 U.S. at 760 (accepting *arguendo* that respondent had a "reasonable expectation of privacy in the text messages sent on the pager provided to him by the City").

185. *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (reasoning that the third-party doctrine is "ill suited to the digital age"); *see also Quon*, 560 U.S. at 759–60 (noting that the Court may "have difficulty predicting how . . . privacy expectations will be shaped . . . or the degree to which society will be prepared to recognize those expectations as reasonable").

186. City of Ontario v. Quon, 560 U.S. 746, 760 (2010).

187. *Id.* at 750.

"necessary for a noninvestigatory work-related purpose."[188] Although the Court's decision involved a non-investigatory search and the actual content of text messages[189] as opposed to metadata, the Court's statements on reasonable expectations of privacy and their dynamic nature were extremely important.[190]

First, it is noteworthy that the Court assumed, *arguendo*, that the respondent had a reasonable expectation of privacy in the texts sent and received from his work-related device and stored with a third party.[191] While an *arguendo* assumption has no legal effect, it does suggest the proposition is one the Court does not find unreasonable.[192] Second, the Court noted that it must "proceed with care" on issues of electronic communications and privacy due to the "[r]apid changes" in technology and what "society accepts as proper behavior."[193] While the Court's admonitions were dicta, they do show the Court recognized the ever-changing nature of electronic communications and societal expectations of privacy, and may be willing to adjust its doctrines—or the third-party doctrine in particular—accordingly.[194]

2. Re-Thinking the Third-Party Doctrine: *United States v. Jones*

Despite its musings about the fluctuating nature of technology and reasonable expectations of privacy, the Court in *Quon* did not directly question then-existing norms or the third-party doctrine.[195] However, two years later in *United States v. Jones*,[196] the validity of the third-party doctrine was openly questioned in Justice Sotomayor's concurring opinion.[197] Further, four Justices concluded that virtually constant, omnipresent surveillance would "impinge[] on expectations of privacy."[198]

In *Jones*, the Supreme Court had to decide whether the government's warrantless attachment of a GPS device to an individual's car was a search or seizure under the Fourth Amendment.[199] The Court

188. *Id.* at 761 (quoting O'Connor v. Ortega, 480 U.S. 709, 726 (1987) (plurality opinion)).
189. *See id.*
190. *See id.* at 759–61.
191. *See id.* at 750, 760.
192. *See id.* at 760.
193. *Id.* at 759.
194. *See id.* at 759–60.
195. *See id.*
196. United States v. Jones, 565 U.S. 400 (2012).
197. *See id.* at 417(Sotomayor, J., concurring).
198. *Id.* at 430 (Alito, J., concurring).
199. *Id.* at 402 (majority opinion).

held that the installation of the GPS in order to surveil a suspect was a search within the meaning of the Fourth Amendment because the government "physically occupied" a constitutionally protected area in order to gather information.[200]

Interestingly, the two concurring opinions of Justice Sotomayor and Justice Alito were more important than the majority opinion of the Court.[201] Justice Sotomayor opened her opinion by noting that surveillance no longer required "physical intrusion"[202] and that even short-term GPS monitoring can offer significant information about a person's "familial, political, professional, religious, and sexual associations."[203] She next discussed the government's ability to store and mine this information and how this capacity had the potential to "chill[] associational and expressive freedoms."[204] Justice Sotomayor then openly questioned whether the third-party doctrine was still a coherent concept in a time where people cannot help but "reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[205] Justice Sotomayor concluded her opinion by again calling into question the premise of the third-party doctrine,[206] and noted that she did not think Americans would unprotestingly accept the government having warrantless access to so much personal information.[207]

In Justice Alito's concurring opinion, which was joined by Justices Ginsburg, Breyer, and Kagan, he noted how dramatic changes in technology could alter society's expectations of privacy.[208] He distinguished the "short-term monitoring of a person's movements" in public from "longer term GPS" surveillance, stating that the latter "impinges on expectations of privacy."[209] To Justice Alito, the length of the surveillance, and the corresponding breadth and depth of the information yielded, was crucial because reasonable people would not expect that law enforcement could keep up such surveillance.[210] As such, according to Justice Alito, lengthy GPS monitoring that could "catalogue

200. *See id.* at 404–05.
201. *See generally id.* at 413–18 (Sotomayor, J., concurring); *id.* at 418–31 (Alito, J., concurring).
202. *Id.* at 414 (Sotomayor, J., concurring).
203. *Id.* at 415.
204. *Id.* at 415–16.
205. *Id.* at 417.
206. *See Jones*, 565 U.S. at 418 (Sotomayor, J., concurring) ("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.").
207. *Id.*
208. *Id.* at 427 (Alito, J., concurring).
209. *Id.* at 430.
210. *See id.*

every single movement" of a person was a search within the meaning of the Fourth Amendment.[211]

Although the concurring opinions of Justices Sotomayor and Alito came in the context of a case involving extensive GPS surveillance, their shared concern revolves around omnipresent surveillance.[212] For Justice Sotomayor, this concern took the shape of questioning the continued validity of the third-party doctrine in an age when people are constantly generating heaps of metadata about their private lives while completing everyday tasks.[213] For Justices Alito, Ginsburg, Breyer, and Kagan, this concern dealt with lengthy government surveillance that could "catalogue" a person's every move.[214] It seems likely, based on the logic of the concerns expressed regarding GPS metadata, that these same concerns would apply to the metadata created by electronic communications.[215]

Perhaps just as noteworthy in *Quon* and the *Jones* concurrences was the recognition that society's expectations of privacy are fluid and can change, sometimes dramatically, with the advent of new technologies.[216] The recognition of the dynamic nature of societal expectations of privacy and its relationship to technological change by at least six Justices of the now-sitting Court[217] makes it quite possible that the Court, with the right case, could revisit and do away with the third-party doctrine. A re-examination of the third-party doctrine, which provides the legal foundations for § 2709, could potentially end the FBI's use of NSLs.

---

211. *See id.* at 430–31.

212. *See id.* at 417 (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring).

213. *Id.* at 417 (Sotomayor, J., concurring).

214. *Id.* at 430–31 (Alito, J., concurring).

215. *See* SCHNEIER, *supra* note 11, at 24. According to Schneier:

> Telephone metadata alone reveals a lot about us. The timing, length, and frequency of our conversations reveal our relationships with others . . . . Phone metadata reveals what and who we're interested in and what's important to us, no matter how private. It provides a window into our personalities

Id.

216. *See* City of Ontario v. Quon, 560 U.S. 746, 759 (2010); *see also Jones*, 565 U.S. at 427 (Alito, J., concurring).

217. *See Quon*, 560 U.S. at 759 (warning that the Court should "proceed with care" on issues of electronic communications and privacy due to the "[r]apid changes" in technology and what "society accepts as proper behavior"); *see also Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (stating that it "may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" as "[t]his approach is ill-suited to the digital age"); *id.* at 429-30 (Alito, J., concurring) (arguing that the legislature is better suited to balance "dramatic technological change . . . privacy concerns" and "changing public attitudes").

B. The Lower Courts: Bound by the Third-Party Doctrine

Despite the Supreme Court's recent skepticism regarding the coherence of the third-party doctrine in the 21st century,[218] lower courts have overwhelmingly continued to employ the third-party doctrine with regard to non-content data.[219] Numerous lower courts have adjudicated various issues regarding warrantless government requests for individuals' non-content data, including requests for historical cell-site location data,[220] IP address data,[221] and to/from address data.[222] In deciding these cases, lower courts have continually declared that *Smith* is binding precedent and these forms of metadata fall under the third-party doctrine.[223] Importantly, these courts have placed great emphasis on the fact that the non-content data was voluntarily and willingly "exposed" by the individuals to the third-party companies.[224] In short, lower courts have generally considered themselves bound by the third-party doctrine,[225] have placed a great deal of importance on the fact that non-content data was involved,[226] and have stressed that individuals have voluntarily transferred this information to the third parties.[227]

Although the lower federal courts have generally considered *Smith* to be binding precedent, there has been disagreement in some federal

---

218. *See supra* Section III.A.1–.2.

219. *See* United States v. Graham, 824 F.3d 421, 424, 427–28 (4th Cir. 2016) (en banc); United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016).

220. *See Graham*, 824 F.3d at 427–28 (concluding that no Fourth Amendment violation occurred where the government obtained historical cell-site location records from cell phone service providers because the defendants did not have a reasonable expectation of privacy in information they willingly "exposed" to the cell phone company).

221. *See* United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010) (determining that the defendant had no expectation of privacy in his IP address because an IP address is voluntarily turned over to a third party and therefore cannot establish a Fourth Amendment violation).

222. *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) ("[E]-mail and internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for . . . directing the routing of information.").

223. *See Graham*, 824 F.3d at 427 ("The Supreme Court's reasoning in *Smith* controls."); *Carpenter*, 819 F.3d at 888 ("Thus, for the same reasons that Smith had no expectation of privacy in the numerical information at issue there, the defendants have no such expectation in the locational information here. On this point, *Smith* is binding precedent.").

224. *See Graham*, 824 F.3d at 427; *Christie*, 624 F.3d at 574.

225. *See, e.g.*, *Carpenter*, 819 F.3d at 888.

226. *See, e.g.*, *id.* at 886 ("[F]ederal courts have long recognized a core distinction: although the content of personal communications is private, the information necessary to get those communications from point A to point B is not.").

227. *See Graham*, 824 F.3d at 427; *Christie*, 624 F.3d at 574.

courts,[228] and dissention in some state courts, regarding how voluntarily cell phone users give their data to third parties.[229] In the Fourth Circuit, in a case that was later reheard *en banc* and found to be governed by *Smith*, the court initially found that individuals did have a reasonable expectation of privacy in certain non-content data.[230] Similarly, in 2010, the Third Circuit, which later found *Smith* controlling in non-content data cases,[231] initially agreed that cell phone users did not "voluntarily" expose their location data to their service providers, and really did not "voluntarily expose[] anything at all."[232] However, despite sporadic decisions to the contrary in lower federal courts and some disagreement by state courts,[233] lower courts have largely found themselves bound by

228. *See* United States v. Graham, 796 F.3d 332, 344–45 (4th Cir. 2015), *aff'd on other grounds on reh'g en banc*, 824 F.3d 421 (4th Cir. 2016); *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317–18 (3d Cir. 2010).

229. *See* Zanders v. State, 58 N.E.3d 254, 263, 266 (Ind. Ct. App. 2016), *aff'd in part*, 73 N.E.3d 178 (Ind. Sup. Ct. 2017); State v. Lunsford, 141 A.3d 270, 271 (N.J. 2016).

230. *See Graham*, 796 F.3d at 344–45. The court held that:

> [T]he government conducts a search under the Fourth Amendment when it obtains and inspects a cell phone user's historical CSLI [(historical cell-site location data)] for an extended period of time. Examination of a person's historical CSLI can enable the government to trace the movements of the cell phone and its user across public and private spaces and thereby discover the private activities and personal habits of the user. Cell phone users have an objectively reasonable expectation of privacy in this information. Its inspection by the government, therefore, requires a warrant, unless an established exception to the warrant requirement applies.

Id.

231. *See Christie*, 624 F.3d at 574.

232. *In re Application*, 620 F.3d at 317–18. The court stated that:

> A cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way. As the [Electronic Frontier Foundation] notes, it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all."

Id. (quoting Amicus Brief for EFF at 21, *In re Application*, 620 F.3d 304 (No. 08-4227)).

233. *See Zanders*, 58 N.E.3d at 263, 266 (holding that the defendant had a reasonable expectation of privacy in historical cell phone location data and that the third-party doctrine as articulated under *Miller* and *Smith* did not apply to this data stored by his cell phone provider because a cell phone user does not convey this information "voluntarily or otherwise" to a third party and therefore "does not assume any risk of disclosure to law enforcement"); *Lunsford*, 141 A.3d at 271 ("[T]his Court has departed from federal law and recognized that, under the New Jersey Constitution, individuals have a reasonable expectation of privacy in information they provide to phone companies, banks, and Internet service providers in order to use commercial services.").

Smith and the third-party doctrine.[234]

C. Do NSLs Violate the Fourth Amendment?

The continuing viability of the third-party doctrine is relevant to NSLs because the FBI is able to use NSLs to get individuals' metadata from CSPs because of the third-party doctrine.[235] Without the third-party doctrine, the FBI's use of NSLs is a violation of the Fourth Amendment's probable cause and warrant requirements.[236] Based on the previously-discussed *Quon* and *Jones* cases,[237] the Supreme Court should modernize its Fourth Amendment jurisprudence and reevaluate the applicability of the third-party doctrine to 21st century communications technology.[238] Once it does so, it will become clear that the FBI's use of NSLs violates the Fourth Amendment.

1. Why the Third-Party Doctrine No Longer Makes Sense and the Use of NSLs Without It Violates the Fourth Amendment

Without the third-party doctrine, the FBI's use of NSLs would be an unreasonable search under the Fourth Amendment *Katz* test.[239] Courts that have employed the third-party doctrine have placed great emphasis on the fact that non-content data was involved, under the assumption that non-content data is less informative,[240] and have stressed that individuals have voluntarily transferred this information to the third parties.[241] However, both of these assumptions are flawed, and when considered in their true light, show the FBI's use of NSLs to be unreasonable searches under the Fourth Amendment.[242]

As pointed out by Stewart Baker, a former NSA general counsel, "[m]etadata absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content."[243] In *Jones*, Justice

234. *See* United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) (en banc); United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016).

235. *See* 18 U.S.C. § 2709 (2012).

236. *See* U.S. CONST. amend. IV.

237. *See supra* Section III.A.1–.2.

238. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

239. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

240. *See* Smith v. Maryland, 442 U.S. 735, 741–42 (1979); United States v. Carpenter, 819 F.3d 880, 886 (6th Cir. 2016).

241. *See* United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016); United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010).

242. *See* United States v. Jones, 565 U.S. 400, 415–17 (2012) (Sotomayor, J., concurring).

243. SCHNEIER, *supra* note 11, at 27.

Sotomayor expressed a similar concern about omnipresent surveillance, noting how even short-term GPS monitoring could reveal a great deal about an individual's life and associations.[244] In fact, in 2012, researchers in the United Kingdom were able to determine within 20 meters where an individual would be 24 hours later using only cell phone tracking data.[245] When metadata is aggregated, it can paint a stunningly accurate picture of who we are.[246] In short, having access to metadata makes having access to content unnecessary.[247]

The key underlying premise of the third-party doctrine, which is that individuals voluntarily give their metadata to CSPs, is just as flawed as the assumption that non-content data is less informative than content data. As Justice Marshall noted in his dissent in *Smith*, "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[248] It is not a controversial claim to state that in the 21st century, an individual can hardly function in modern society without access to the Internet and a cell phone.[249] Because an individual must use the Internet and a cell phone to carry out everyday tasks, and generates vast quantities of metadata about himself or herself while doing so, it cannot seriously be contended that an individual is voluntarily disclosing this information to a third party.[250]

Once the assumptions about the voluntariness and uninformative nature of metadata are dispelled, it becomes clear that the FBI's use of NSLs is an unreasonable search under the Fourth Amendment *Katz* test.[251] First, Americans have a subjective expectation of privacy in their metadata because they do not believe the government should be able to obtain their metadata from third parties without probable cause or a warrant.[252] Second, based on how personally revealing metadata can be[253] and the fact that an individual has virtually no choice but to

244. *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring).

245. SCHNEIER, *supra* note 11, at 2 (citing Manlio De Domenico, Antonio Lima & Mirco Musolesi, *Human Mobility Prediction: Predicting Human Mobility Using Mobile Phone Data*, UNIV. BIRMINGHAM (June 2012), http://www.cs.bham.ac.uk/research/projects/nsl/mobility-prediction).

246. *See id.* at 24–27.

247. *See id.* at 27.

248. Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

249. *See* Wei Chen Lin, Comment, *Where Are Your Papers?: The Fourth Amendment, the Stored Communications Act, the Third-Party Doctrine, the Cloud, and Encryption*, 65 DEPAUL L. REV. 1093, 1114–16 (2016).

250. *See id.* at 1114.

251. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (articulating the test for an unreasonable search as violating an individual's subjective expectation of privacy and an objective expectation of privacy society considers reasonable).

252. *See* Lin, *supra* note 249, at 1121.

253. *See* SCHNEIER, *supra* note 11, at 27.

constantly produce endless amounts of metadata,[254] this expectation of privacy in one's metadata should be one society considers reasonable. Without the third-party doctrine, the FBI's use of NSLs becomes an unreasonable search under the Fourth Amendment.[255]

2. The Fourth Amendment Applies Through the State Action Requirement's Entanglement Exception

The Fourth Amendment applies to the FBI's use of NSLs through the entanglement exception to the state action requirement.[256] Although CSPs are collecting and storing the metadata of their customers, which would ordinarily not involve the Fourth Amendment because of the state action requirement,[257] the Fourth Amendment is implicated once these CSPs begin turning the metadata over to the government.[258] The Fourth Amendment becomes applicable because of the entanglement exception, which states that state action exists where the government "affirmatively authorizes, encourages, or facilitates unconstitutional action."[259]

When the FBI issues an NSL to a CSP, the FBI is not only "affirmatively authoriz[ing], encourag[ing], or facilitat[ing] unconstitutional action,"[260] but is also actively coercing CSPs to turn over the private data of citizens under threat of criminal prosecution.[261] If the government was itself collecting, storing, and using the personal information of individuals in criminal investigations and prosecutions, the Fourth Amendment would undoubtedly be implicated.[262] When the FBI issues an NSL to a CSP, the same collection, storage, and use of personal information is occurring, except the government is able to skirt the Fourth Amendment via the third-party doctrine by having the CSP collect the data and then using the "full coercive power of government"[263] to obtain the data. There is insufficient justification as to why NSLs cannot comply with the probable cause and warrant requirements of the Fourth Amendment, and the Court should not be involved in maintaining a doctrine that allows the government to

254. *See* Lin, *supra* note 249, at 1114–16.
255. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).
256. *Cf.* Chemerinsky & Schwartz, *supra* note 92, at 780.
257. *See* United States v. Stanley, 109 U.S. 3, 17 (1883).
258. *See id.* at 13.
259. *See* Chemerinsky & Schwartz, *supra* note 92, at 780.
260. *Id.*
261. *See* 18 U.S.C. § 2709 (2012).
262. *See* U.S. CONST. amend. IV.
263. *See* Shelley v. Kraemer, 334 U.S. 1, 19 (1948).

circumvent the Constitution.[264] As such, the Fourth Amendment and its probable cause and warrant requirements should apply to NSLs.[265]

IV. CONCLUSION

The Supreme Court should reevaluate the third-party doctrine in light of 21st century technology and in the spirit of Justice Sotomayor in *United States v. Jones*.[266] The third-party doctrine did not cohere to the practical realties of modern life when it was first promulgated,[267] and is completely incoherent today.[268] In the 21st century, individuals have virtually no choice but to use the Internet and cell phones, which in turn generate and "reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[269] Individuals rightly have a subjective expectation of privacy in their metadata and similarly, this expectation is one that society should recognize as reasonable.[270] What is not reasonable is the government having access to this highly personal information without meeting the probable cause and warrant requirements of the Fourth Amendment.[271] The Supreme Court should not maintain a doctrine that allows the government to flaunt constitutional mandates.[272]

While several authors have called for the re-evaluation or more limited application of the third-party doctrine,[273] the third-party doctrine should instead be abolished altogether. Further, the Supreme Court should subject NSLs to the probable cause and warrant requirements of the Fourth Amendment.[274] Currently, there are at least six Justices who are troubled by omnipresent surveillance and who may be willing to

264. *See* U.S. CONST. amend. IV.
265. *Id.*
266. *See supra* Section III.A.2.
267. *See* Smith v. Maryland, 442 U.S. 735, 749–50 (1979) (Marshall, J., dissenting). According to Justice Marshall:

> [U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. . . . It is idle to speak of "assuming" risks in contexts where, as a practical matter, individuals have no realistic alternative.

Id. (citations omitted).
268. *See* Lin, *supra* note 249, at 1114–16.
269. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).
270. See *supra* Section III.C.1–.2; *see also,* Lin, *supra* note 249, at 1121.
271. *See supra* Section III.C.1–.2.
272. *See supra* Section III.C.2.
273. *See* Aaron Stevenson, *A Fourth Amendment Framework for the Future: Applying the Mosaic Theory to Digital Communications*, 77 OHIO ST. L.J. FURTHERMORE 145, 147 (2016); Lauren Doney, Comment, *NSA Surveillance,* Smith *& Section 215: Practical Limitations to the Third-Party Doctrine in the Digital Age*, 3 NAT'L SEC. L.J. 462, 469 (2015).
274. *See supra* Section III.C.1–.2.

reevaluate the third-party doctrine and modernize the Court's Fourth Amendment jurisprudence.[275] To effectuate this change, the Court should either take up a case where a CSP challenges compliance with an NSL or in order to avoid a standing issue, a case where an individual challenges the government's use of metadata acquired from a CSP.[276]

In deciding such a case, the Court would be able to, and should, do four things: (1) abolish the third-party doctrine as incoherent in the 21st century; (2) find that the FBI's use of NSLs falls under the Fourth Amendment through the entanglement exception to the state action requirement; (3) find that individuals have both a subjective and objective expectation of privacy in their metadata; and (4) hold that the use of NSLs by the FBI under § 2709 is unconstitutional because it does not comply with the probable cause and warrant requirements of the Fourth Amendment and does not fall under any of the exceptions to those requirements.[277] By taking these steps, the Court would be able to modernize its Fourth Amendment jurisprudence and do away with a doctrine that allows the government to circumvent the Constitution and invade the privacy rights of Americans.

275. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring); *id.* at 427 (Alito, J., concurring); City of Ontario v. Quon, 560 U.S. 746, 759 (2010).

276. *See* United States v. Carpenter, 819 F.3d 880, 886 (6th Cir. 2016), *cert granted*, 137 S. Ct. 2211 (2017). Although the Court has not yet issued its decision, the case should give the Court an excellent chance to re-assess the applicability of the third-party doctrine in the 21st century. One commentator, trying to read the tea leaves from oral argument, tweeted that "plainly the Court is much more concerned about the privacy implications of new technology today than it was five years ago." Amy Davidson Sorkin, *In Carpenter Case, Justice Sotomayor Tries to Picture the Smartphone Future*, NEW YORKER (Nov. 30, 2017), https://www.newyorker.com/news/our-columnists/carpenter-justice-sotomayor-tries-to-picture-smartphone-future.

277. *See supra* Section III.C.1–.2.

***