A NEW THIRD-PARTY DOCTRINE: THE TELEPHONE METADATA PROGRAM AND *CARPENTER V. UNITED STATES*

*Mary-Kathryn Takeuchi**

Introduction

The third-party doctrine was long considered a well-established principle that was not going anywhere anytime soon. It traces back to early Fourth Amendment jurisprudence in 1967, when the Supreme Court issued its landmark decision in *Katz v. United States*.[1] There, the Court asserted that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[2] The Court affirmed this assertion in *United States v. Miller*, holding that checks and other financial records voluntarily turned over to a bank were not subject of Fourth Amendment protection,[3] and again in *Smith v. Maryland*, holding that phone numbers dialed out were voluntarily conveyed to a phone company and therefore not entitled to Fourth Amendment protection.[4] What resulted was a bright-line rule that guided courts in deciding cases under the third-party doctrine: an individual has no reasonable expectation of privacy under the Fourth Amendment in information that is voluntarily conveyed to a third party.[5]

---

* Mary-Kathryn ("Katie") Takeuchi, Juris Doctor Candidate, Notre Dame Law School, 2020; Bachelor of Arts in Economics, The George Washington University, 2016. I express my most sincere thanks to Professor Jimmy Gurulé for providing valuable guidance that has been integral not only to the writing of this Note, but to my entire law school career. I would also like to thank the members of the *Notre Dame Law Review* for their thorough editing and constant encouragement. All errors are my own.

1 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (explaining the holding to be that the Fourth Amendment protects that in which "a person has a . . . reasonable expectation of privacy").

2 *Id.* at 351 (majority opinion).

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

4 Smith v. Maryland, 442 U.S. 735, 744 (1979).

5 *See id.* at 742 ("[The court] doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial . . . realiz[ing] that they must 'convey' phone numbers to the telephone company."); *Miller*, 425 U.S. at 442 (explaining that there is "no legitimate 'expectation of privacy' in . . . information voluntarily conveyed to the banks and exposed to their employees"); *see also Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

In 2018, the Supreme Court confronted and reconsidered the forty-year-old third-party doctrine in the newest Fourth Amendment landmark case, *Carpenter v. United States*.[6] The digital world—a world in which technology and mobile devices are extensions of our own bodies, tracking our every conversation, every move, every purchase, every internet search—was becoming one in which the bright-line rule of voluntary disclosure could no longer thrive. Would the Court allow these tiny 5.8-inch devices that captivate Americans' entire lives in sixty-four gigabits to reveal such personal information to the government without a warrant? Chief Justice Roberts, writing for the majority, recognized these concerns and made a substantial retreat from the traditional bright-line approach of the third-party doctrine.[7] What came from the *Carpenter* decision was a new balancing test that weighs the reduced or reasonable expectation of privacy against whether the information was truly voluntarily exposed to the third party.[8]

Roberts asserted that the Court's decision in *Carpenter* should have no bearing on national security law.[9] By making that simple assertion, however, he raised the red flag and called attention to the question of how the third-party doctrine applies to the collection of information relating to national security. Perhaps the most significant question is how the third-party doctrine applies to bulk metadata collection under the Foreign Intelligence Surveillance Act's telephone metadata program. Under the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, the government could collect and record any tangible thing, most significantly, bulk telephone metadata on millions of Americans without a warrant.[10] In an infamous 2013 leak to the press, the American public discovered that the government had collected and recorded bulk metadata on millions of wireless subscribers.[11] Congress attempted to remedy the situation by enacting new legislation. However, the impact of the new law remains unclear, with millions of datapoints still being collected and recorded, which has long been defended by the fact that individuals turn over revealing information to their wireless providers, thereby barring them from bringing any Fourth Amendment claim against the government.[12]

This Note will answer the question of whether bulk metadata collection is still defensible under the third-party doctrine. It ultimately concludes that

6 138 S. Ct. 2206 (2018).

7 *See id.* at 2220 (holding that the third-party doctrine did not apply to CSLI data).

8 *See id.* at 2219–20 (applying the balancing test); *see also id.* at 2231 (Kennedy, J., dissenting) ("The Court appears, in my respectful view, to read *Miller* and *Smith* to establish a balancing test. For each 'qualitatively different category' of information, the Court suggests, the privacy interests at stake must be weighed against the fact that the information has been disclosed to a third party.").

9 *Id.* at 2220 (majority opinion) ("[O]ur opinion does not consider other collection techniques involving foreign affairs or national security.").

10 *See infra* notes 100–01 and accompanying text.

11 *See infra* notes 102–03 and accompanying text.

12 *See infra* Part II (describing in depth the issues surrounding bulk metadata collection).

Roberts incorrectly asserted that *Carpenter* will not impact the application of the third-party doctrine to collection techniques involving national security, and that the warrantless collection of bulk metadata under the Foreign Intelligence Surveillance Act is no longer defensible by the third-party doctrine. In Section I.A, this Note discusses traditional Fourth Amendment jurisprudence in *Katz v. United States* and the establishment of the third-party doctrine as a bright-line rule in *United States v. Miller* and *Smith v. Maryland*. This Note also provides background on the Court's hint at a coming change in the third-party doctrine in *United States v. Jones*.[13] In Section I.B, this Note explains the Court's decision in *Carpenter v. United States* before laying out the new balancing test in Section I.C. In Part II, this Note describes the issue at hand by discussing the controversy surrounding bulk metadata collection under the Foreign Intelligence Surveillance Act's telephone metadata program, as well as the open question remaining of whether the government's collection under that program is defensible by the third-party doctrine. In Part III, this Note applies *Carpenter*'s new balancing test to the telephone metadata program and determines that, because individuals have a reasonable expectation of privacy in the metadata collected by the government under the telephone metadata program, and that because there is no voluntary exposure, the privacy interests at stake clearly outweigh the mere fact that information has been disclosed to wireless carriers. As such, the Note concludes that the telephone metadata program constitutes Fourth Amendment activity because the third-party doctrine no longer protects the government from defending warrantless searches. Section III.D also briefly discusses the implications of the findings under the new balancing test and suggests how courts will further evaluate the constitutionality of bulk metadata collection.

I. Background

In order to understand the substantial retreat from the third-party doctrine that the Supreme Court made in *Carpenter v. United States*, this Note begins by reviewing the origins of Fourth Amendment jurisprudence. Section I.A provides a summary of *Katz v. United States* and then explains the establishment of the third-party doctrine in *United States v. Miller* and *Smith v. Maryland*, which was later questioned in *Jones v. United States*. This Part then proceeds to describe the Supreme Court's decision in *Carpenter* and the resulting emergence of a new balancing test.

13 565 U.S. 400 (2012).

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

1. *Katz v. United States*: A Reasonable Expectation of Privacy

The Fourth Amendment protects the principle that "a person has a . . . reasonable expectation of privacy."[14] Modern Fourth Amendment jurisprudence can be traced back to these words in the Supreme Court's decision in *Katz*, where it rejected the idea that something might be a "constitutionally protected area," and rather asserted that "the Fourth Amendment protects people, not places."[15] In that case, the government overheard Katz's conversation from outside of a public telephone booth and used the content of that conversation as evidence against him in a criminal proceeding.[16] The Court held that Katz had a reasonable expectation of privacy in his conversation, and that "[t]he [g]overnment's activities in electronically listening to and recording [Katz's] words violated the privacy upon which he justifiably relied while using the telephone booth."[17] As such, the Court held that the government's activities in *Katz* constituted a Fourth Amendment search and seizure.[18] However, the Court also determined that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[19] This foreshadowed what would soon become known as the third-party doctrine.

2. *United States v. Miller* and *Smith v. Maryland*: Establishing the Third-Party Doctrine

Almost a decade after the *Katz* decision, in *United States v. Miller*,[20] Mitch Miller was convicted of operating an undocumented whiskey distillery in

---

14 Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (agreeing with the Court's holding in this aspect).

15 *See id.* at 350–51 (majority opinion) (noting that the Court "decline[s] to adopt this formulation of the issues").

16 *See id.* at 348 (describing the government's attempt "to introduce evidence of [Katz's] end" of the conversation "overheard by FBI agents who had attached" a listening device to the phone booth).

17 *Id.* at 353.

18 *Id.* ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."). This Note will refer to Fourth Amendment searches and seizures as "Fourth Amendment activity." After determining that Katz had a reasonable expectation of privacy, the Court conducted the second part of its Fourth Amendment two-step test, addressing "whether the search and seizure conducted in this case complied with constitutional standards." *See id.* at 354–59. This Note focuses only on what is considered Fourth Amendment activity, so only the first part of the Court's Fourth Amendment two-step test is relevant to the Note's analysis.

19 *Id.* at 351.

20 425 U.S. 435 (1976).

Kathleen, Georgia.[21] While investigating the case, the government obtained copies of checks and other financial records without a warrant.[22] Miller alleged that this constituted unlawful Fourth Amendment activity, but the Court determined that Miller had no protectable Fourth Amendment interest in the checks and financial records.[23] The Court relied on *Katz* in finding that there was "no legitimate 'expectation of privacy,'" as Miller had voluntarily conveyed the information to the banks and their employees—a third party.[24] The Court in *Miller* drew a bright-line rule for the third-party doctrine: when information is voluntarily conveyed to a third party, there is no legitimate expectation of privacy and, therefore, no Fourth Amendment interest in the information. Therefore, there is no Fourth Amendment activity, and the individual lacks standing. The Court's determination was a bright-line rule as it made its decision without inquiry into *how* voluntary the conveyance of information was, or if there still remained any legitimate, or reasonable, expectation of privacy in the information.

The Court affirmed its reasoning in *Miller* and the bright-line rule of the third-party doctrine in *Smith v. Maryland*.[25] In that case, a robbery victim called the police, reporting that the man identifying himself as the robber had repeatedly made threatening phone calls to the victim following the robbery.[26] During one of the phone calls, the man told the victim to step outside. In doing so, the victim saw the man driving slowly past her home.[27] Using the information provided by the victim, the government was able to trace the license plate number on the car to Michael Smith.[28] The government, without a warrant, directed Smith's telephone company to install a pen register that would record the numbers dialed from his home.[29] The pen register revealed that Smith was calling the victim, and using this information, the government then secured a warrant that revealed evidence supporting a charge and conviction for robbery.[30] Smith argued that the installation and use of the pen register violated his Fourth Amendment rights.[31] The

21 *Id.* at 437 (describing the facts of the case where the sheriffs discovered the illegal distilleries after a fire broke out at the warehouse that Miller rented).

22 *Id.* at 436 (explaining that the government obtained records "by means of . . . subpoenas *duces tecum* served upon two banks at which [Miller] had accounts.").

23 *Id.* at 440 (finding that "there was no intrusion into any area in which [Miller] had a protected Fourth Amendment interest").

24 *Id.* at 442 ("[W]e perceive no legitimate 'expectation of privacy' in their contents. . . . All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.").

25 442 U.S. 735 (1979).

26 *Id.* at 737.

27 *Id.*

28 *Id.*

29 *Id.*

30 *Id.*

31 *Id.* at 742 ("Given a pen register's limited capabilities, . . . petitioner's argument that its installation and use constituted a 'search' necessarily rests upon a claim that he had a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone.").

Court rejected Smith's claim.[32] The Court held that, under the third-party doctrine, Smith had no reasonable expectation of privacy because he voluntarily conveyed the phone numbers he dialed to his phone company, which the Court considered a third party.[33] Relying on *Miller*, the Court employed an assumption of the risk reasoning to support the bright-line rule in the third-party doctrine.[34]

3. *United States v. Jones*: Questioning the Third-Party Doctrine

The Supreme Court's 2012 decision in *United States v. Jones*[35] led to the questioning of the viability of the third-party doctrine in the modern world. After Antoine Jones came under suspicion of trafficking narcotics, the government installed a GPS-tracking device on his vehicle while it was publicly parked.[36] For the following four weeks, the government tracked the vehicle's movements, which revealed more than two thousand pages of data.[37] This data supported an indictment to charge Jones with conspiracy to distribute and possess with intent to distribute cocaine.[38] The district court allowed the admission of this evidence, holding that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[39] This reasoning follows from the third-party doctrine and the idea that an individual automatically has no reasonable expectation of privacy in information shared, even if not directly shared with a third party but rather shared through the use of public roads. The court of appeals reversed the lower court's decision, holding that the government's actions constituted Fourth Amendment activity and violated the Fourth Amendment.[40] The Supreme Court affirmed.[41] The Court pointed to the pervasiveness of the four-week-long tracking, noting that such "longer term" GPS tracking implicated a reasonable expectation of privacy.[42]

---

32 *Id.*

33 *Id.* ("[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 the telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.").

34 *Id.* at 744 ("Because the depositor 'assumed the risk' of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private.").

35 565 U.S. 400 (2012).

36 *See id.* at 402–03.

37 *Id.* at 403.

38 *Id.*

39 United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006) (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)).

40 *See Jones*, 565 U.S. at 404.

41 *Id.* at 413.

42 *See id.* at 412.

The Court also noted that by attaching the GPS-tracking device to a private area—the vehicle—the government "encroached on a protected area."[43]

In her concurrence, Justice Sotomayor, recognizing that much of the government's argument stemmed from the third-party doctrine (although it was in no way a perfect application), suggested 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."[44] Sotomayor noted that the third-party doctrine is "ill suited to the digital age," pointing to modern use of technology and the amount of information individuals store on mobile devices simply in "the course of carrying out mundane tasks."[45] She rejected the assumption 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."[46] Sotomayor's refusal to accept that an individual has no reasonable expectation of privacy in information simply because of the mere fact that she shared it with a third party set the stage for the Court's decision in *Carpenter* six years later.

B. Carpenter v. United States

In 2011, four men were arrested for robbing Radio Shack and T-Mobile stores.[47] One of the suspects identified fifteen accomplices and provided their cell phone numbers to the government.[48] The prosecutors used this information to obtain cell phone records from wireless carriers for several other suspects, including Timothy Carpenter.[49] The cell-site location information (CSLI) data provided the government with 12,898 location points for Carpenter alone.[50] This information supported a charge of six counts of robbery and six counts of carrying a firearm during a federal crime of violence.[51] Carpenter filed a motion to suppress the CSLI data provided by the wireless carriers, arguing that the government's warrantless seizure of the CSLI data was an unlawful Fourth Amendment search unsupported by probable

43 *Id.* at 410.

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

45 *Id.* ("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.").

46 *Id.* at 418.

47 Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

48 *Id.*

49 *Id.* The prosecutors were able to obtain such information by applying for a court order under the Stored Communications Act, which "permits the Government to compel the disclosure of certain telecommunications records when it 'offers specific and articulable facts showing that there are reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.'" *Id.* (quoting 18 U.S.C. § 2703(d) (2012)).

50 *Id.* For a description of how CSLI data works, see *id.* at 2211.

51 *Id.* at 2212.

cause.[52] The trial court denied Carpenter's motion.[53] At trial, the information placed Carpenter at four of the robberies.[54] This supported multiple convictions and a sentence of over 100 years in prison.[55] The Sixth Circuit affirmed the trial court's decision based on its well-founded understanding of the third-party doctrine.[56] The Supreme Court granted a writ of certiorari.[57]

The Court determined that the government violated Carpenter's Fourth Amendment rights when it accessed CSLI data from his wireless carriers, and held that the third-party doctrine did not apply to the facts in *Carpenter*.[58] *Carpenter* is a substantial retreat from the Court's historical application of the third-party doctrine, in that the Court now qualifies and considers the level of (1) the individual's expectation of privacy and (2) the individual's voluntary exposure.[59] Thus, a new balancing test emerged from this decision, though the majority never called it such. Rather Justice Kennedy, in dissent, understood the Court's reasoning to be a balancing test, which requires that "the privacy interests at stake must be weighed against the fact that the information has been disclosed to a third party."[60] Justice Kennedy further noted that only "[w]hen the privacy interests are weighty enough to 'overcome' the third-party disclosure, [will] the Fourth Amendment's protections apply."[61] This significantly departs from previous Fourth Amendment jurisprudence, which treated the third-party doctrine as a bright-line rule.[62]

---

52 *Id.*

53 *Id.*

54 *Id.* at 2212–13. "In the Government's view, the location records clinched the case . . . ." *Id.* at 2213.

55 *Id.* ("Carpenter was convicted on all but one of the firearm counts and sentenced to more than 100 years in prison.").

56 *See id.* ("The court held that Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers. Given that cell phone users voluntarily convey cell-cite data to their carriers as 'a means of establishing communication,' the court concluded that the resulting business records are not entitled to Fourth Amendment protection." (quoting Smith v. Maryland, 442 U.S. 735, 741 (1979))).

57 *Id.*

58 *See id.* at 2220 ("[The Court] decline[s] to extend *Smith* and *Miller* to the collection of CSLI" because "the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection.").

59 *See id.* at 2219–20 (discussing in depth the two rationales underlying the third-party doctrine: a reduced expectation of privacy and voluntary exposure).

60 *Id.* at 2231 (Kennedy, J., dissenting).

61 *Id.* at 2232.

62 The bright-line rule comes from *Miller* and *Smith* and articulates that an individual does not automatically have a reasonable expectation of privacy in that which she shares with a third party. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) (doubting that "people in general entertain any actual expectation of privacy in the numbers they dial . . . realiz[ing] that they must 'convey' phone numbers to the telephone company"); United States v. Miller, 425 U.S. 435, 442 (1976) (ruling that there is "no legitimate 'expectation of privacy' in . . . information voluntarily conveyed to the banks and exposed to their employees"); *see also* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly

C. Carpenter*'s New Balancing Test*

1. Factor One: A Reasonable or Reduced Expectation of Privacy

The first factor in determining applicability of the third-party doctrine is whether there is a "reasonable" or "reduced" expectation of privacy.[63] In making such determination of privacy interests in *Carpenter*, the Court considered "'the nature of the particular documents sought' to determine whether 'there is a legitimate[64] "expectation of privacy" concerning their contents.'"[65] This is a substantial retreat from the notion "that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[66] Instead, an individual's expectation of privacy is placed on a spectrum and falls either into a realm of reasonable or reduced.

The Court took two steps in determining whether there is a reasonable or reduced expectation of privacy. First, in considering the nature of the documents, the Court looked at limitations on the information available. In doing so, the Court distinguished the facts of *Carpenter* from those of *Smith*, noting that the capabilities of a pen register are limited.[67] Telephone call logs do not reveal content that might be considered "identifying information."[68] However, the Court acknowledged that there are no such limitations on the CSLI data in *Carpenter*.[69] The time-stamped CSLI data provides insight to the intimate details of an individual's life including one's location, but also going so far as to reveal "familial, political, professional, religious, and sexual associations."[70] Furthermore, it cannot even be said that there is a limitation on *whose* information is collected, as the CSLI data continuously logs information for the 400 million cell phone devices belonging to everyone in the United States, rather than just those individuals under investigation.[71]

---

exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

63 *Carpenter*, 138 S. Ct. at 2219 ("The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another.").

64 In *Carpenter*, the Court apparently equates "legitimate" to "reasonable." The Court has also used the word "actual" in its previous decisions when discussing the expectation of privacy. I read all three to have the same meaning, and I employ the use of the word "reasonable" in this Note.

65 *Carpenter*, 138 S. Ct. at 2219 (quoting *Miller*, 425 U.S. at 442).

66 *Smith*, 442 U.S. at 743–44.

67 *See Carpenter*, 138 S. Ct. at 2219 (citing *Smith*, 442 U.S. at 742).

68 *Id.* (quoting Riley v. California, 573 U.S. 373, 400 (2014)).

69 *See id.* at 2219 (discussing the government's failure to recognize that there are no comparable limitations).

70 *Id.* at 2217 (quoting *Riley*, 573 U.S. at 396).

71 *Id.* at 2218 ("Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone.").

Second, in determining whether there is a reasonable or reduced expectation of privacy in such documents, the Court examined the pervasiveness of the government's actions.[72] In *Carpenter*, the Court placed special emphasis on the retrospective pervasiveness of CSLI data. There, the Court explained that the "detailed chronicle" of a person's every movement "compiled every day, every moment, over several years" was so pervasive as to implicate a reasonable expectation of privacy.[73] Furthermore, the retrospective pervasiveness of the "*historical* cell-site records,"[74] along with the societal norm that individuals "compulsively carry cell phones with them all the time,"[75] led the Court to analogize the level of surveillance made possible by a cell phone to that of an ankle monitor.[76] The Court recognized that this allows the government to "*travel back in time* to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers, which currently maintain records for up to five years."[77] The Court considered the CSLI to provide the wireless carriers with an infallible memory.[78] The Court placed a similar emphasis on pervasiveness in *Jones*, where it stated that the "longer term" GPS tracking of a vehicle implicated a reasonable expectation of privacy.[79] Because CSLI data has a "unique nature" that implicates privacy concerns similar to—or even beyond—those in *Jones*, the Court held that an individual has a reasonable expectation of privacy in the record of his physical movements captured by CSLI data.[80]

2. Factor Two: Voluntary Exposure

The second factor at hand involves finding out whether there was a voluntary exposure of the information to a third party.[81] Again, the Court took two steps to determine whether there was voluntary exposure. First, the

72 *See id.* at 2220.

73 *Id.*

74 *Id.* at 2218 (emphasis added).

75 *Id.*

76 *See id.* ("Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.").

77 *Id.* (emphasis added).

78 *Id.* at 2219 ("[The wireless carriers] are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible.").

79 *Id.* at 2220 (citing United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment)) ("But when confronted with more pervasive tracking, five Justices agreed that longer term GPS monitoring of even a vehicle traveling on public streets constitutes [Fourth Amendment activity]."). The Court also noted that the tracking of CSLI data is even more pervasive than the tracking of a vehicle. *Id.* at 2218 ("While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time.").

80 *Id.* at 2217 ("[A]n individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI [data].").

81 *See id.* at 2220 (discussing "the second rationale underlying the third-party doctrine—voluntary exposure").

information must truly be shared.[82] Second, there must be some affirmative act that allowed the individual to opt into sharing the information.[83] This is a substantial retreat from the Court's previous and consistent holding "that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[84] Instead, the Court adopted the stance taken from the dissent in *Smith*, which would require that an individual actively make the choice to share the information in order to trigger the third-party doctrine.[85]

In the first step, the Court looks at whether the individual has a choice in the recording of the information. If there is no choice, then the Court is reluctant to find that the information is truly shared. In *Carpenter*, the Court noted that cell phones are "indispensable to participation in modern society."[86] As such, almost everyone in the United States owns one, and the Court points out that "[o]nly the few without cell phones could escape this tireless and absolute surveillance."[87] With cell phones being considered such a necessity to individuals in the United States, the Court concluded that CSLI data conveyed to wireless carriers through them "is not truly 'shared' as one normally understands the term."[88]

In the second step, the Court considered assumption of the risk through some affirmative act made by the individual.[89] In *Carpenter*, the Court did not find that Carpenter had assumed any risk because the recording of CSLI data is triggered through "[v]irtually any activity on the phone."[90] Short of disconnecting from the network, the Court reasoned that an individual has "no way to avoid leaving behind a trail of location data."[91] Therefore, the Court determined that Carpenter did not assume of the risk of turning over a "comprehensive dossier of his physical movements" simply through operating a cell phone.[92] Without anything further, the Court appears unlikely to find voluntary exposure.

---

82 *See id.*

83 *See id.*

84 Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

85 *See id.* at 749 (Marshall, J., dissenting) ("Implicit in the concept of assumption of risk is some notion of choice.").

86 *Carpenter*, 138 S. Ct. at 2220.

87 *Id.* at 2218.

88 *Id.* at 2220.

89 *See id.* ("Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user . . . ."). Such "affirmative act" is likely what Justice Marshall would consider to be a "choice" in his dissent in *Smith*. It is significant that this differs from how Justice Blackmun discussed assumption of the risk in *Smith*. *See supra* notes 84–85 and accompanying text.

90 *Carpenter*, 138 S. Ct. at 2220.

91 *Id.*

92 *Id.*

3. Balancing the Factors

Finally, the Court weighed "the privacy interests at stake . . . against the fact that the information ha[d] been disclosed to a third party."[93] It concluded that the mere fact that the government was able to collect the information from the wireless carrier—a third party—was insufficient to overcome the reasonable expectation of privacy in the CLSI data.[94] The balancing test in *Carpenter* was simple: there was no truly voluntary exposure of the CSLI data to outweigh Carpenter's reasonable expectation of privacy in the information.[95] As such, the Court concluded that the government's collection constituted a Fourth Amendment search.[96]

II. THE ISSUE

In this Part, this Note looks in depth at the issue of the government's bulk metadata collection. It begins with a summary of the telephone metadata program under the Foreign Intelligence Surveillance Act and the controversial leak to the public about the government's collection. It then discusses the failed Fourth Amendment challenge brought before the Supreme Court, the legislation enacted in an attempt to mitigate privacy concerns, and the remaining conclusion that the bright-line rule guiding the third-party doctrine controls cases regarding the telephone metadata program's constitutionality.

The Foreign Intelligence Surveillance Act of 1978[97] ("FISA") established the Foreign Intelligence Surveillance Court (FISC), which reviews government requests for orders allowing electronic surveillance.[98] FISA allowed the government to obtain orders from the FISC that would allow the government to collect business records, so long as there were "specific and articulable facts" indicating that the business records related to foreign intelligence and international terrorism investigations.[99] Following the terrorist attacks of September 11, 2001, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("PATRIOT Act").[100] Section 215 of the PATRIOT Act

93 *Id.* at 2231 (Kennedy, J., dissenting); *see also id.* at 2220 (majority opinion) (balancing the factors).

94 *Id.* at 2220 ("[T]he fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection.").

95 *See supra* subsections I.C.1–.2.

96 *See Carpenter*, 138 S. Ct. at 2220 ("The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.").

97 Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801–1811 (2012)).

98 *See* GEOFFREY CORN ET AL., NATIONAL SECURITY LAW 199 (2015).

99 *Id.* at 211.

100 Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered titles of the U.S. Code).

amended FISA to allow for not just the collection of business records, but also of "any tangible things."[101]

In 2013, *The Guardian* published information leaked by Edward Snowden, a 29-year-old former CIA employee, exposing the National Security Agency's telephone metadata program that was collecting records of millions of Verizon subscribers in the United States.[102] Relying on section 215 of the PATRIOT Act, under the telephone metadata program, wireless carriers provided to the government originating and terminating telephone numbers, as well as the time and duration of the calls.[103] Such information was maintained in a database and stored for five years.[104] The revelation of the telephone metadata program raised privacy concerns, as the government's collection "would allow the NSA to build easily a comprehensive picture of who any individual contacted, how and when, and possibly from where, retrospectively."[105]

The American Civil Liberties Union (ACLU) responded by filing suit against the government.[106] The ACLU alleged both that section 215 does not authorize the telephone metadata program, and that even if it does, it violates the Fourth Amendment.[107] The Second Circuit decided that because the telephone metadata program was not authorized by statute, it did not need to address the constitutional issue.[108] However, the court of appeals noted that the Fourth Amendment issue was "potentially vexing."[109] The government contended that the telephone metadata program did not constitute Fourth Amendment activity under the third-party doctrine.[110]

101 *Id.* § 215, 115 Stat. at 287–88. The PATRIOT Act allows the government to "make an application for an order requiring the production of any tangible thing[ ] . . . for an investigation to protect against international terrorism or clandestine intelligence activities." *Id.*

102 Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; *see also* Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (revealing Edward Snowden as the individual who leaked the information).

103 *See* CORN ET AL., *supra* note 98, at 212–13 (explaining the telephone metadata program).

104 *Id.* at 212.

105 Greenwald, *supra* note 102.

106 ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).

107 *See id.* at 821 (introducing the constitutional claim as an alternative argument).

108 *See id.* at 824 ("Because we conclude that the challenged program was not authorized by the statute on which the government bases its claim of legal authority, we need not and do not reach these weighty constitutional issues.").

109 *Id.* at 821.

110 *See id.* at 822 (discussing the government's argument that the third-party doctrine requires the rejection of the appellants' claim that the telephone metadata program "violates the Fourth Amendment, or even implicates its protections at all").

The ACLU argued for a revisitation of the third-party doctrine.[111] While the court offered some discussion on the matter, it never provided an answer.[112]

In 2015, Congress enacted the United and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 ("FREEDOM Act").[113] The FREEDOM Act was aimed at ending the telephone metadata program under section 215.[114] Under the FREEDOM Act, the government can no longer directly collect and maintain the phone records of U.S. citizens.[115] Rather, the government must now seek warrants from the FISC that will allow it to direct wireless carriers to turn over data on their subscribers.[116] However, the enactment of the FREEDOM Act has not done away with the telephone metadata program, or any of the privacy concerns that come with it.[117] For example, Executive Order 12,333 could be construed to allow for the telephone metadata program to collect and store communications by persons from the United States without a warrant.[118] Furthermore, when Larry Klayman filed an emergency petition for a rehearing en banc for his case concerning the constitutionality of the telephone metadata program, the D.C. Circuit denied his petition, and then-Judge Kavanaugh wrote in his concurring statement:

> I vote to deny plaintiffs' emergency petition for rehearing en banc. I do so because, in my view, the Government's metadata collection program is entirely consistent with the Fourth Amendment. . . . The Government's collection of telephony metadata from a third party such as a telecommunica-

111 *See id.* ("Appellants respond that modern technology requires revisitation of the underpinnings of the third-party records doctrine as applied to telephone metadata.").

112 *See id.* at 821–25; *see also id.* at 824 ("[W]e need not and do not reach these weighty constitutional issues.").

113 Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (codified as amended in scattered sections of 12, 15, 18, and 50 U.S.C).

114 *See id.* Additionally, the PATRIOT Act was set to expire when the FREEDOM Act was enacted. *See* Steven Nelson, *Senate Passes Freedom Act, Ending Patriot Act Provision Lapse*, U.S. NEWS & WORLD REP. (June 2, 2015), https://www.usnews.com/news/articles/2015/06/02/senate-passes-freedom-act-ending-patriot-act-provision-lapse.

115 *See* Robert Hackett, *No, NSA Phone Spying Has Not Ended*, FORTUNE (Dec. 1, 2015), http://fortune.com/2015/12/01/nsa-phone-bulk-collection-end/ ("Congress eventually reacted by replacing parts of the [PATRIOT Act], which authorized the privacy-invasive program, with a seemingly-less-intrusive piece of legislation, the [FREEDOM Act], over the summer.").

116 *See id.* (discussing the new process for obtaining telephone metadata under the FREEDOM Act).

117 *See generally id.* (noting and further explaining how "[i]t would be wrong to conclude, however, that this moment signaled the demise of the agency's surveillance powers" and further asserting that "questions remain about [the FREEDOM Act's] implementation").

118 Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981); *see also* John Napier Tye, Opinion, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, WASH. POST (July 18, 2014), https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html?noredirect=on&utm_term=.18c29fa1b489.

> tions service provider is not considered a search under the Fourth Amendment, at least under the Supreme Court's decision in *Smith v. Maryland*. That precedent remains binding on lower courts in our hierarchical system of absolute vertical stare decisis.[119]

There is significant uncertainty surrounding the government's telephone metadata program stemming from the end of the PATRIOT Act to Kavanaugh's assertion that it remains constitutional. Kavanaugh's concurring opinion was written *after* the FREEDOM Act passed. It signaled that bulk metadata collection still occurs, and that the government's collection of it could be defended by the third-party doctrine. In fact, Kavanaugh's statement proved that the question of its constitutionality under the Fourth Amendment could not even be tested simply because the metadata is turned over to wireless carriers. And the resulting problem at hand is this: the NSA has continued to collect millions of records about Americans' phone calls under the telephone metadata program.[120] Those collected and recorded data points far outnumber the number of warrants granted to the NSA.[121] There is little transparency surrounding that matter.[122] However, it is significant that the government announced that it had not been collecting bulk metadata in recent months, and that President Trump may not ask Congress to renew its legal authority when it expires at the end of the year.[123] Regardless, courts cannot answer the question of whether the telephone metadata program is constitutional so long as *Miller* and *Smith* guide the courts in determining that under the bright-line rule of the third-party doctrine, because the metadata is shared with wireless carriers, the government's collection of it is not considered Fourth Amendment activity.

This is in no way a new problem. In his dissenting opinion in *Miller*, Justice Brennan expressed concern about Congress creating programs that allow the government access to information "without invocation of the judi-

---

119 Klayman v. Obama, 805 F.3d 1148, 1148–49 (D.C. Cir. 2015) (Kavanaugh, J., concurring in the denial of rehearing en banc) (citation omitted). Judge Kavanaugh draws a superficial comparison between the metadata program and the facts of *Smith*, relying mostly on the fact that both information sets came from the use of a telephone, and ignoring entirely the substantial change from the use of phones when *Smith* was decided in contrast to the current way that society uses phones and mobile devices. His assertion that the lower court is bound by that case almost invites the Supreme Court to decide otherwise.

120 *See* James Vincent, *NSA Collected 151 Million Phone Records in 2016, Despite Surveillance Law Changes*, VERGE (May 3, 2017), https://www.theverge.com/2017/5/3/15527882/nsa-collecting-phone-records-us-citizen-metadata.

121 *See id.*

122 *See id.*

123 *See* Charlie Savage, *Disputed N.S.A. Phone Program is Shut Down, Aide Says*, N.Y. TIMES (Mar. 4, 2019), https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html. It is fair to be skeptical of the government's assertion that it will stop metadata collection. Even as the article points out, after the replacement system under the FREEDOM Act took effect, "the scale of collection remained huge." *Id.*; *see also* Vincent, *supra* note 120.

cial process"[124]—which is exactly what occurs with the telephone metadata program. Congress freely creates and undoes the government's ability to access information, while the courts are unable to address its constitutionality so long as the courts cannot recognize it as Fourth Amendment activity. Most significantly, dating back to *Katz*, Justice Douglas saw the new direction of Fourth Amendment jurisprudence as "a wholly unwarranted green light for the Executive Branch to resort to electronic eavesdropping without a warrant in cases which the Executive Branch itself labels as 'national security' matters,"[125] seemingly foreshadowing today's problem.

However, the Court's new third-party balancing test in *Carpenter* might just help us solve it.

III. ANALYSIS

Since the *Carpenter* decision, no court has answered the question of the constitutionality of the telephone metadata program. Prior to *Carpenter*, courts ruled that the telephone metadata program was constitutional under *Miller* and *Smith*.[126] In light of the Supreme Court's decision in *Carpenter*, courts would apply *Carpenter*'s balancing test, rather than the bright-line rule in *Miller* and *Smith*. The *Carpenter* balancing test makes a substantial retreat from past historical understandings of the third-party doctrine. This Note applies the new balancing test from *Carpenter* and finds that in its application, the third-party doctrine no longer extends to the telephone metadata program. As such, this Note suggests that the government's collection of telephone metadata likely constitutes Fourth Amendment activity and opens up the opportunity for the Supreme Court to rule on its constitutionality under the Fourth Amendment.

A. Factor One: Individuals Have a Reasonable Expectation of Privacy in the Metadata Collected by the Government Under the Telephone Metadata Program

In applying *Carpenter*'s new third-party balancing test, courts will need to take the same two steps as the Supreme Court did in determining whether a reasonable or reduced expectation of privacy exists in the metadata collected by the government under the telephone metadata program. Much of the analysis here will appear similar to the Court's analysis in *Carpenter*. Courts will likely find a reasonable, rather than reduced, expectation of privacy in the information collected under the telephone metadata program for the following reasons.

---

124 United States v. Miller, 425 U.S. 435, 453 (1976) (Brennan, J., dissenting).

125 Katz v. United States, 389 U.S. 347, 359 (1967) (Douglas, J., concurring).

126 *See supra* note 119 and accompanying text.

1. The Metadata Is Not Limited

The Court in *Carpenter* first examined the limitations on the information available during the collection of CSLI data.[127] Here, courts will likely find that the telephone metadata program reveals nearly unlimited amounts of information. Especially given that the government can access originating and terminating telephone numbers, as well as the time, location, and duration of the calls, much can be inferred from telephone metadata without insight into the content of a call, "such as where people work and where people live."[128] It is relatively simple to track the movements of an individual using telephone metadata.[129] For example, in one study, a team was able to "uniquely pinpoint" the location information of ninety-five percent of their subjects from merely four records of the location and time of each call.[130] Information about the content of the call is unnecessary.[131] The NSA could then "cross-referenc[e]" this information with other data such as "credit card transactions or e-mail communications" to reveal more information about an individual.[132] Such cross-referencing has the potential to "reveal sensitive activity such as attendance at a particular church or a visit to an abortion clinic."[133] This raises concerns similar to those that the Court expressed in *Carpenter*—that the information could reveal the intimate details about an individual's life including "familial, political, professional, religious, and sexual associations."[134] Similarly, courts will likely reach a similar conclusion that there further lacks limitations on whose information is collected; the *Carpenter* Court placed emphasis on the fact that the CSLI data "tracking capacity r[an] against everyone."[135] As such, courts will most likely find that the information collected under the telephone metadata program lacks limitations, which will weigh in favor of individuals having a reasonable expectation of privacy.

127 Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

128 Jessica Leber, *Mobile Call Logs Can Reveal a Lot to the NSA*, MIT TECH. REV. (June 18, 2013), https://www.technologyreview.com/s/516181/mobile-call-logs-can-reveal-a-lot-to-the-nsa/. Leber further bolsters her point by arguing that because of "how much the NSA could glean from call records," it is misleading to downplay the significance of metadata collection. *Id.*

129 *See id.* (discussing Vincent Blondel's study in which his team analyzed fifteen months of anonymous call records from 1.5 million people and could pinpoint movements of ninety-five percent of people from only four records using the location and time of each call).

130 *Id.*

131 *See id.* (Blondel stating in an interview that, "[y]ou can infer a lot, such as where people work and where people live . . . [without] information about the content").

132 *Id.*

133 *Id.*

134 Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

135 *Id.* at 2218.

2. The Telephone Metadata Program Is Pervasive

Next, the *Carpenter* Court considered the pervasiveness of CSLI data collection. Here, courts will likely find that the telephone metadata program is so pervasive as to implicate an individual's reasonable expectation of privacy in the information that the government collects. The pervasiveness is similar to that which the Court found in *Carpenter*.[136] Nearly indistinguishable from the "detailed chronicle" of location information in *Carpenter*,[137] the telephone metadata also creates a detailed chronicle by collecting the time of calls, the calls' locations, and the calls' durations. As mentioned in the previous point, such insight into an individual's communication can allow for the government to understand a significant amount about an individual's life. Furthermore, the pervasiveness is retrospective, as the government collects and maintains the information for five years. This retrospective pervasiveness—as compared to CSLI data[138]—has an infallible memory, tracing and recording every number dialed in and out, how long the call lasted, and from or to where the call was made. Therefore, the "detailed chronicle" of information revealed by the bulk metadata program is also "compiled every day, every moment, over several years."[139] As such, courts will most likely find that the information collected under the telephone metadata program to be especially pervasive, which weighs in favor of individuals having a reasonable expectation of privacy.

B. Factor Two: There Is No Voluntary Exposure

In further applying *Carpenter*'s new third-party balancing test, courts additionally will need to take the same two steps as the Supreme Court in determining whether individuals voluntarily expose the metadata to the wireless carriers merely by using their services. This analysis again mirrors the Court's analysis in *Carpenter*. It is unlikely that courts will find voluntary exposure for the following reasons.

1. The Metadata Is Not "Truly Shared" with Wireless Carriers

The *Carpenter* Court first considered whether the individual had a meaningful choice in the recording of the metadata.[140] When no choice existed, the Court was reluctant to find that information was truly shared.[141] Here, courts will likely find no meaningful choice, and therefore, that the information collected under the telephone metadata program is not truly shared. In *Carpenter*, the Court noted that cell phones are "indispensable to participa-

136 *See id.* at 2220.
137 *Id.*
138 *See id.* (emphasizing that this pervasiveness is especially concerning when it details "a person's physical presence compiled every day, every moment, over several years").
139 *Id.*
140 *See id.*
141 *See id.*

tion in modern society."[142] The same is true here. Because the use of cell phones is "indispensable," the only way to avoid surveillance under the telephone metadata program is to not use a cell phone.[143] This is an impractical solution, given that ninety-two percent of Americans own cell phones,[144] and that Americans also have an "intimate relationship" with them.[145] Cell phones have not only become commonplace, but a necessary staple to most individuals. Therefore, because cell phones are such a necessity in everyday life to the point that their use is unavoidable, the information that they transmit to wireless carriers cannot reasonably be considered " 'shared' as one normally understands the term."[146] These considerations weigh against courts finding voluntary exposure.

2. Individuals Do Not "Assume the Risk" Through an Affirmative Action

Finally, the Court in *Carpenter* evaluated whether individuals assumed the risk of their CSLI data being collected and recorded.[147] Here, courts will most likely find that individuals do not assume the risk of their information being recorded and stored under the telephone metadata program by some affirmative act. Under the telephone metadata program, any incoming or outgoing call—arguably the primary purpose of a cell phone—would trigger the recording of information. Not only are incoming and outgoing calls the primary purpose of a cell phone, but cell phones are becoming the only way that Americans make and receive calls. Studies show that 50.8% of American households no longer have a landline telephone, but rather, at least one member of the household owns a cell phone.[148] Moreover, 50.5% of all adults and 60.7% of all children live in homes that only have cell phones.[149]

142 *Id.*

143 In *Carpenter*, the Court already accepted this statement as true. *See id.* at 2218. ("Only the few without cell phones could escape this tireless and absolute surveillance.").

144 Monica Anderson, *Technology Device Ownership: 2015*, PEW RES. CTR. (Oct. 29, 2015), http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/.

145 *See* Lesley Alderman, *The Phones We Love Too Much*, N.Y. TIMES (May 2, 2017), https://www.nytimes.com/2017/05/02/well/mind/the-phones-we-love-too-much.html (explaining this intimate relationship by the fact that we sleep with, eat with, and always keep our cell phones with us). Alderman notes that Americans check their phones, on average forty-seven times a day, and suggests that number might increase to eighty-two times a day among younger populations. *See id.* Americans' attachment to their cell phones can be explained by the fact that "[t]hey tell us the weather, the time of day and the steps we [have] taken. They find us dates (and sex), entertain us with music and connect us to friends and family," and "[t]hey answer our questions and quell feelings of loneliness and anxiety." *Id.*

146 *Carpenter*, 138 S. Ct. at 2220.

147 *See id.* ("Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up.").

148 STEPHEN J. BLUMBERG & JULIAN V. LUKE, NAT'L CTR. FOR HEALTH STATISTICS, WIRELESS SUBSTITUTION: EARLY RELEASE OF ESTIMATES FROM THE NATIONAL HEALTH INTERVIEW SURVEY, JULY–DECEMBER 2016, at 1 (2017), https://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201705.pdf.

149 *Id.*

Such information means that individuals do not alternate between a cell phone and landline telephone usage; they do not borrow phones to make or receive calls; they do not check their voicemail remotely or use pay phones. Everything is being done from one central device: the cell phone. Just like in *Carpenter*, where the Court noted that "[v]irtually any activity on the phone generates CSLI," courts must recognize that any activity done on the phone (and there are many of them) generates the information collected under the telephone metadata program.[150] Furthermore, similar to how the Court noted that "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data," courts must account for the fact that an individual could only turn off the phone in order prevent metadata from being collected and recorded.[151] The use of a cell phone, which is an act so ingrained in Americans' daily activities that it simply cannot be thought of as an affirmative action, turns over a "comprehensive dossier" of calls from which significant information can be inferred.[152] This will also weigh against the courts finding voluntary exposure.

C. Balancing the Factors

Justice Kennedy correctly described that the final step courts must take involves a balancing test. Courts must weigh "the privacy interests at stake . . . against the fact that the information has been disclosed to a third party."[153] In doing so here, courts will likely find that: (1) individuals have a reasonable expectation of privacy in the information collected by the government under the telephone metadata program; and (2) even though that information is turned over to wireless carriers through the use of cell phones, it cannot reasonably be said that individuals are making a voluntary exposure of such information. Therefore, the privacy interests at stake clearly outweigh the mere fact that information has been disclosed to the wireless carriers. Courts must then find that *Miller* and *Smith* no longer control such cases and that the telephone metadata program constitutes Fourth Amendment activity. Courts will finally be able to answer the question of whether the government violates individuals' Fourth Amendment rights.

D. Implications of the Balancing Test Findings

The fact that the third-party doctrine most likely no longer extends to the telephone metadata program does not automatically mean that the government's collection of metadata is unconstitutional. Rather, it means that individuals can now bring constitutional challenges to the government's warrantless searches under FISA because those individuals will no longer lack

150 *Carpenter*, 138 S. Ct. at 2220.

151 *Id.*

152 This is like the "comprehensive dossier" of location information, which CSLI data reveals. *Id.*

153 *Id.* at 2231 (Kennedy, J., dissenting).

standing.[154] From this point, courts will consider whether the warrantless search was supported by probable cause that the individual was engaged in criminal activity that constituted a national security threat.[155] This further testing by the courts will require a more fact-specific inquiry.

Due to the lack of transparency surrounding the current collection of telephone metadata under FISA, it is difficult to know what query terms the government uses, on what grounds they query, and how many individuals they reach under a suspicion of a single person.[156] These factors will all hold significant weight with courts as they decide whether the government had probable cause to conduct a warrantless search. Moreover, if the laws change again and Congress enacts a bill with a provision similar to section 215 of the PATRIOT Act, the government could easily return to unlimited warrantless searching.[157] Some of those searches may be justified, while others most certainly will not. The uncertainly and lack of transparency makes any kind of prediction of how the courts will rule far too speculative. One thing, however, remains clear under the application of *Carpenter*'s new balancing test to the telephone metadata program: the courts will give us an answer on the constitutionality of bulk metadata collection very soon.

Conclusion

The new balancing test introduced by the Court in *Carpenter v. United States*[158] marks a substantial retreat from our traditional understanding of the Fourth Amendment in *Katz v. United States*,[159] and our understanding of the

154 The Court in *Carpenter* explains this, noting that "[h]aving found that the acquisition of Carpenter's CSLI was a search," it could now go on to test the search's constitutionality under the Fourth Amendment and "conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records." *Id.* at 2221 (majority opinion). This comes from the Court's original understanding of testing the constitutionality of the government's action under the Fourth Amendment in *Katz*. Katz v. United States, 389 U.S. 347 (1967). In order to find a violation of the Fourth Amendment, the Court required, first, that the government's actions constituted a search or seizure, which is what this Note has referred to as "Fourth Amendment activity." *Id.* at 353 ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."). After finding Fourth Amendment activity, "[t]he question remaining for decision, then, is whether the search and seizure conducted in th[e] case complied with constitutional standards." *Id.* at 354.

155 *See Katz*, 389 U.S. at 357 (requiring a probable cause justification).

156 *See* Vincent, *supra* note 120 (noting that millions of records continue to be disproportionately collected by the government with respect to the number of warrants granted, without explanation).

157 *See* United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287–88 (codified as amended at 50 U.S.C. §§ 1861–1863 (2012)).

158 138 S. Ct. 2206 (2018).

159 389 U.S. 347 (1967).

third-party doctrine in *United States v. Miller*[160] and *Smith v. Maryland*.[161] It addresses Justice Sotomayor's concerns about the third-party doctrine's place in a modernizing digital world, as she explained in her concurrence in *United States v. Jones*.[162] And it returns to the question prompted by Justice Douglas in his dissent in *Katz* of how we handle abuses of Fourth Amendment jurisprudence that are masked as national security concerns.[163]

The third-party doctrine is no longer guided by a bright-line rule. Courts must now balance whether there is a reasonable or reduced expectation of privacy in information against whether that information is truly shared. Despite Chief Justice Roberts's protests that *Carpenter* was a narrow holding, the new balancing test has serious implications that reach issues within national security law. Specifically, the new balancing test would apply to the telephone metadata program as it applied to the collection of CSLI data. Under the telephone metadata program, the government collected bulk telephone metadata from millions of American wireless users, an action previously defensible simply because Americans turn over that information to their wireless carriers. The implications of the FREEDOM Act on this behavior is unclear, as it effectively ended bulk collection under section 215 of the PATRIOT Act. But significant collection still occurs, transparency on the matter is limited, and the number of data points collected far exceeds the number of warrants granted. Even with the government's assertion that data collection will come to an end, the true problem lies in that the Supreme Court has never ruled that bulk metadata collection violates the Fourth Amendment. In light of *Carpenter*, that question now has the opportunity to be considered.

When that question reaches the Supreme Court, the Justices will likely find that the third-party doctrine does not bar a Fourth Amendment claim because the third-party doctrine will no longer apply. First, the Court will most likely find that individuals have a reasonable expectation of privacy in the metadata collected by the government under the telephone metadata program. This is (1) because the metadata is not limited, as it reveals nearly unlimited information that can be inferred without the content of the calls; and (2) because the telephone metadata program is pervasive, as it provides retrospective insight to the past five years of an individual's life. Second, the Court will most likely find that there is no voluntary exposure. There is no voluntary exposure because the metadata is not truly shared with wireless carriers as cell phones have a necessary and common place in everyday life and because individuals do not assume the risk through an affirmative action, as they need do nothing more than simply start up their phone in order to

160 425 U.S. 435 (1976).

161 442 U.S. 735 (1979).

162 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

163 *Katz*, 389 U.S. at 359 (Douglas, J., concurring) (viewing the Fourth Amendment jurisprudence at the time as giving a "wholly unwarranted green light for the Executive Branch to resort to electronic eavesdropping without a warrant in cases which the Executive Brach itself labels 'national security' matters").

trigger the sharing of information. The reasonable expectation of privacy in the telephone metadata is buttressed by the fact that there is no voluntary exposure of the information. With the determination that the bulk metadata collection constitutes Fourth Amendment activity and the telephone metadata is entitled to Fourth Amendment protection, courts can finally answer the question of whether the government's collection of such information violates the Fourth Amendment—a question that will surely reach the Supreme Court in the near future.