Science and Technology Law Review

Volume 21 | Number 2 Article 7

2018

Alexa, Give My Personal Information to the Government: The Application of the Third-Party Doctrine to Smart Devices

Brandon Pieratt
Southern Methodist University, Dedman School of Law, bpieratt@smu.edu

Alexa, Give My Personal Information to the Government: The Application of the Third-Party Doctrine to Smart Devices

*Brandon Pieratt**

I. INTRODUCTION

Imagine a world in which you can control nearly everything with a voice command or the tap of a thumb. "Alexa, start my car." "Siri, turn on my lights for the evening." The rate at which we are developing new technology far surpasses the rate at which we are adapting the law to match. In 1986, less than half of one percent of Americans owned cellular phones.[1] In 1994, only nine percent of Americans owned cellular phones.[2] As of 2016, ninety-five percent of Americans owned cellular phones.[3] Ownership of smart devices is also on the rise.[4] According to research, one in six adults in the United States, around thirty-nine million Americans, owns a voice-activated smart device.[5] "Additionally, thirty-one percent of smart speaker owners are asking their virtual assistants to control other devices in the home, with sixty-one percent controlling devices in the living room and thirty-eight percent controlling devices in the kitchen."[6] The more technology advances, the more difficult it becomes to protect privacy with existing judicial standards and antiquated statutes.

Under current judicial interpretations, because we are sharing information with third parties, such as Amazon through the Echo device, the data shared is not granted Fourth Amendment protection.[7] This is due to the continued use of the third-party doctrine, which essentially eliminates any reasonable expectation of privacy for information that is voluntarily conveyed to

---

* Brandon Pieratt is a 2019 candidate for a Juris Doctor from SMU Dedman School of Law. He received a Bachelor of Business Administration from Midwestern State University in Wichita Falls, Texas.

1. *See* CTIA, BACKGROUND ON CTIA'S WIRELESS INDUS. SURVEY 2 (2015), https://api.ctia.org/docs/default-source/default-document-library/ctia_survey_ye_2014_graphics.pdf.

2. *See id.* at 2.

3. *See Mobile Facts Sheet*, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/.

4. *See* Ryan Browne, *Adoption of Voice-Activated Speakers is Now Outpacing that of Smartphones in the US*, CNBC (Jan. 15, 2018), https://www.cnbc.com/2018/01/15/39-million-us-adults-now-own-a-voice-activated-smart-speaker-study.html.

5. *Id.*

6. *Id.*

7. *See generally* United States v. Miller, 425 U.S. 435 (1976).

a third party.[8] This doctrine has been used to allow the warrantless collection of many types of information, including cell phone location data and bank records.[9] More recently, a court in Oregon attempted to obtain recorded data from an Amazon Echo device that was located in the home of a murder suspect.[10] Unfortunately for progress, the issue was never litigated because the defendant agreed to turn over the data voluntarily, so we can only speculate on where the law is headed in this area.[11]

This Comment argues that the current Fourth Amendment protections afforded to data voluntarily conveyed to third parties is inadequate for an age in which nearly all of our information is shared with an outside agent. Accordingly, the Supreme Court must update the doctrine or get rid of it completely. The Court may do this by applying the *Katz* test to each factual situation rather than simply determining that if the information was provided to a third party, it is not protected by the Fourth Amendment. In addition, the Court must reexamine its definition of "voluntary" and further analyze the totality of the circumstances when coming to its conclusions.

Part II of this comment discusses the history of the law as applied to advances in technology. Part III discusses the most current applications of the law. Next, Part IV will give a brief overview of virtual assistants and their relevance. Part V will discuss the proposed solution to the current misapplication of third-party doctrine precedent, and Part VI will discuss the possible problems with the proposed solutions. The Comment will conclude by applying the proposed solution to a hypothetical scenario involving the technologies discussed.

II. THE HISTORY OF THE FOURTH AMENDMENT AND THE LAW SURROUNDING THE THIRD PARTY DOCTRINE

A. The Fourth Amendment

The Fourth Amendment of the U.S. Constitution states:

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, 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.[12]

8. *See id.*

9. *See* United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016); *see also Miller*, 425 U.S. at 435.

10. *See* Haley Edwards, *Alexa Takes the Stand: Listening Devices Raise Privacy Issues*, TIME (May 4, 2017), http://time.com/4766611/alexa-takes-the-stand-listening-devices-raise-privacy-issues/.

11. *See id.*

12. U.S. CONST. amend. IV.

According to the Supreme Court, "the central meaning of the Fourth Amendment is 'reasonableness.'"[13] "Whether a particular search or seizure is reasonable is generally determined by balancing the competing interests at stake—the government's interest in effective law enforcement versus an individual's interest in privacy and personal security."[14] Additionally, several narrowly-defined exceptions to the warrant requirement have been delineated through case law.[15] A warrantless search by police is invalid unless it falls within one of these exceptions.[16] Exceptions to the warrant requirement include searches and seizures incident to a lawful arrest, those yielding contraband in plain view, those in hot pursuit of a fleeing criminal, those limited to a stop-and-frisk based on a reasonable suspicion of criminal activity, those based on probable cause in the presence of exigent circumstances, and those based on consent.[17]

The third-party doctrine, under which "an individual can claim 'no legitimate expectation of privacy' in information that he has voluntarily turned over to a third party,"[18] is a controversial exception that is often criticized but highly influential.[19] The exception has been applied to bank records,[20] credit card statements,[21] employment records,[22] and cell-site location data,[23] among others.[24] The following line of cases mark pivotal moments in the evolution of this controversial exception.

B. *Katz v. United States*

Katz v. United States marks the beginning of the third-party doctrine.[25] In *Katz*, the Court held that the wiretapping of a public phone booth constituted a search and seizure under the Fourth Amendment and therefore re-

13. Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 198 (1993).
14. *Id.* at 199.
15. *See* 68 AM. JUR. 2D *Searches and Seizures* § 114 (2018).
16. *See id.*
17. *See id.*
18. United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016).
19. John P. Collins, *The Third Party Doctrine in the Digital Age*, JUST. ACTION CTR. (2012), http://www.nyls.edu/documents/justice-action-center/student_capstone_journal/cap12collins.pdf [http://perma.cc/CXA7-HLFN].
20. United States v. Miller, 425 U.S. 435, 435 (1976).
21. United States v. Phibbs, 999 F.2d 1053, 1077 (6th Cir. 1993).
22. United States v. Hamilton, 434 F. Supp. 2d 974, 979–80 (D. Or. 2006).
23. United States v. Guerrero, 768 F.3d 351, 359–61 (5th Cir. 2014).
24. *See* Smith v. Maryland, 442 U.S. 735 (1979); *see also* United States v. Forrester, 512 F.3d 500, 504 (9th Cir. 2008).
25. *See generally* Katz v. United States, 389 U.S. 347 (1967).

quired a warrant.[26] This holding is significant because it marks the first time that the Supreme Court did not require a physical intrusion to constitute a search.[27] The Court rejected the government's argument that the actions of its agents "should not be tested by Fourth Amendment requirements" because there was no physical penetration of the phone booth and instead held that the "Fourth Amendment protects people, not places."[28] The Court further held that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[29] Finally, the Court expresses that the reach of the Fourth Amendment is affected, at least in part, by a citizen's reasonable expectation of privacy.[30]

In his concurring opinion, Justice Harlan develops a two-part test that would later be judicially recognized as a staple of Fourth Amendment analysis.[31] The *Katz* test requires "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'" (objective).[32] Harlan emphasizes a personal aspect of privacy and infers that the conduct of an individual can provide the court with evidence of a person's subjective expectation.[33] For instance, in the *Katz* case, Harlan opines that the expectation of privacy can be found in the fact that one who occupies a phone booth "shuts the door behind him, and pays the toll that permits him to place a call" (objective conduct of an individual).[34] "The point is not that the booth is 'accessible to the public' at other times, but that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable" (subjective expectations).[35] *Katz v. United States* shifted Fourth Amendment analysis away from the property-based approach that generally linked privacy protections to the home.[36] The shift to focusing on a person's reasonable expectation of privacy opened the door for another exception to the warrant requirement: the third-party doctrine.

26. *See id.* at 359.

27. *See id.* at 352.

28. *Id.* at 351–52.

29. *Id.* at 351.

30. *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

31. *See id.* at 361.

32. *Id.*

33. *See id.*

34. *Id.*

35. *Katz*, 389 U.S. at 361.

36. *See id.* at 352 (majority opinion).

C. *United States v. Miller*

Third-party doctrine principals began to emerge shortly after the opinion in *Katz*.[37] For instance, in *Couch v. United States*, the Court found that the defendant did not have a reasonable expectation of privacy in documents that were handed over to an accountant who then provided them to the Internal Revenue Service.[38] A few years later, one of the more notable cases that applied third party doctrine principles was heard: *United States v. Miller*.[39] In *Miller*, the defendant kept bank accounts with several banks who then, without being served a warrant, provided the defendant's banking information to the Bureau of Alcohol, Tobacco, and Firearms.[40] At trial, the defendant was found guilty of a number of offenses due to the disclosure of the account information.[41] The appellate court reversed, finding that the bank records should have been suppressed.[42] When reviewed by the Supreme Court, the Court reversed, finding that the defendant had no reasonable expectation of privacy in his bank records because the bank was a third party to which he voluntarily disclosed his affairs when he opened his accounts at the bank.[43]

The Court in *Miller* seems to focus on the voluntariness of the defendant's actions and the sensitivity of the information conveyed.[44] The defendant contended that the records kept by the banks were only made available for limited purposes in which he has a reasonable expectation of privacy.[45] The Court referred to *Katz* when justifying their decision, stating that, although the courts have moved away from property interests, a "search and seizure becomes unreasonable when the Government's activities violate 'the privacy on which a person justifiably relies'" and that "what a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[46] The Court, up to this point, had repeatedly held that information revealed to a third party and then conveyed to the government is not prohibited by the Fourth Amendment *even if* the information is revealed on the assumption that it will be used only for a limited purpose and the confidence in the third party will not be betrayed.[47]

37. *See* Couch v. United States, 409 U.S. 322 (1973).

38. *See id.*

39. *See* United States v. Miller, 425 U.S. 435 (1976).

40. *See id.* at 437–38.

41. *See id.* at 438–39.

42. *See id.* at 439.

43. *See id.* at 442.

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

45. *See id.* at 442.

46. *Id.*

47. *Id.* at 443.

Although it seems the Court had already justified their decision, to bolster their opinion even more, the Court further examined "the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."[48] The Court found that because the information obtained only contained "information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," there was no legitimate expectation of privacy in the bank records.[49] The Court stated that:

> [e]ven if we direct our attention to the original checks and deposit slips, rather than to the microfilm copies actually viewed and obtained by means of the subpoena, we perceive no legitimate 'expectation of privacy' in their contents. The checks are not confidential communications but negotiable instruments to be used in commercial transactions.[50]

If the information were more sensitive, it is difficult to determine, based on the opinion, if the Court would have come to a different conclusion. The sensitivity of the information conveyed continues to be an important part of the Court's analysis when applying the *Katz* test to Fourth Amendment claims.

D. *Smith v. Maryland*

The third-party doctrine was strengthened in *Smith v. Maryland*.[51] In *Smith*, the police requested that the telephone company install a pen register at the central office to record the numbers dialed from the defendant's phone.[52] The police did not get a warrant or a court order before the pen register was installed.[53] The information captured on the pen register led to a warrant to search the defendant's home, which led to the arrest and conviction of the defendant.[54] The Supreme Court granted review to "to resolve indications of conflict in the decided cases as to the restrictions imposed by the Fourth Amendment on the use of pen registers."[55]

Consequently, the Court reinforced the reach of the third-party doctrine. The Court found that the defendant had no legitimate expectation of privacy because he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary

48. *Id.* at 442.

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

50. *Id.*

51. 442 U.S. 735 (1979).

52. *See id.* at 737.

53. *Id.*

54. *See id.*

55. *Id.* at 738.

course of business."[56] Smith argued that because he was not conveying the information to a person with the ability to remember every number but to a machine, which only recorded the numbers because of the pen register device, he had a legitimate expectation of privacy.[57] The Court refused to make the distinction and opined that, because the defendant voluntarily conveyed the information to the phone company which had the ability to record numbers dialed, the defendant "assumed the risk that the information would be divulged to police."[58] The Court came to its conclusion by applying the *Katz* test, highlighting the voluntary nature of the disclosure and the lack of sensitivity of the information obtained.[59] "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."[60] Justice Stewart, in the dissent, was not convinced by this argument.[61] He believed that the "content distinction" was arbitrary and that the numbers dialed from a private telephone are not without content.[62] The "content distinction" will become an important element in third-party doctrine cases in the future.

This line of cases set the stage for the future of Fourth Amendment analysis in the courts. The current application of the third-party doctrine can be troublesome in an age where citizens share nearly all of their information with a third party. Our financial transactions are made through a wire transfer or with the swipe of a card through an electronic system. We send correspondence through email and text message, search for an abundance of information on the internet, and control our music and appliances through voice activated smart devices. All of these platforms are run by third parties with whom we "voluntarily" share our information.

E. *United States v. Forrester*

Around thirty years after *Smith*, the courts seemed to apply the third-party doctrine without much of a change. In *United States v. Forrester*, the government employed various surveillance techniques without a warrant which enabled them to learn the "to and from" addresses of the defendant's email messages, the IP addresses of the websites the defendant visited, and the total volume of information sent to or from his account.[63] The defendant claimed the government's surveillance violated the Fourth Amendment, and

56. *Smith*, 442 U.S. at 744.

57. *See id.* at 745.

58. *Id.*

59. *See id.* at 741–42.

60. *Id.* at 741 (quoting United States v. New York Tel. Co., 434 U.S. 159 (1977)).

61. *Smith*, 442 U.S. at 746 (Stewart, J., dissenting).

62. *See id.* at 748.

63. United States v. Forrester, 512 F.3d 500, 505 (9th Cir. 2008).

the court applied the *Katz* test along with third-party doctrine principles.[64] The Ninth Circuit Court of Appeals found the methods used were indistinguishable from that of the pen register approved in *Smith* and found no reasonable expectation of privacy in the information obtained because "[users] should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."[65] Additionally, the information obtained did not "reveal any more about the underlying contents of communication than do phone numbers."[66]

The *Forrester* court seemed to focus on the significance of the information, a growing theme when courts analyze the third-party doctrine as applied to emerging technologies.[67] The court compared the surveillance of email addresses to the information the government could observe on the outside of physical mail.[68] This mail analogy has been allowed in cases dating back to the nineteenth century.[69] Judge Fisher stated that devices that obtain addressing information and the amount of information sent do not "breach the line between mere addressing and more content-rich information."[70] The distinction between content-rich information and metadata has continued to play a pivotal role in the application of the third-party doctrine.

III. DIALING DOWN THE THIRD-PARTY DOCTRINE

Although the courts have applied the third-party doctrine consistently, there has been a recent trend of carving out exceptions in the application of the doctrine. This is especially true in cases involving current technology that is becoming more prevalent in the lives of Americans, such as email and global positioning system (GPS) location data. Additionally, there have been decisions that are not directly related to the third-party doctrine but have the potential to influence Fourth Amendment application in the future in a way that could restore the privacy protections that the Framers intended.

A. *United States v. Warshak*

In *United States v. Warshak*, the government obtained approximately 27,000 of the defendant's emails from internet service providers without a warrant.[71] The defendant claimed the warrantless "search" of his emails was

64. *See id.* at 509.

65. *Id.* at 510.

66. *Id.*

67. *See id.* at 510–11.

68. *Id.* at 511.

69. *Forrester*, 512 F.3d at 511.

70. *Id.*

71. United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010).

a violation of the Fourth Amendment.[72] The Sixth Circuit Court of Appeals applied the *Katz* test to determine whether there was a reasonable expectation of privacy in a person's emails.[73]

First, the court analyzed the subjective component to determine whether the defendant had a subjective expectation of privacy in the contents of his emails.[74] Because of the "often sensitive and sometimes damning substance of his emails," the court found that the defendant did have a reasonable expectation of privacy.[75] The court then analyzed whether "society is prepared to recognize that expectation as reasonable."[76] The court compared the content of the defendant's emails to the content of letters and telephone calls.[77] The court also recognized the importance of allowing the evolution of Fourth Amendment protections to match the "inexorable march of technological process, or its guarantees will wither and perish."[78] In the end, the court determined that both elements of the *Katz* test were met, creating a reasonable expectation of privacy in the contents of the defendant's emails.[79]

The court in *Warshak* was not without reservations.[80] The Justices acknowledged that a subscriber agreement may be written in a manner that is enough to waive the reasonable expectation of privacy.[81] They noted that the ability or right of access of the third party was not enough to overcome the reasonable expectation of privacy, but, if an internet service provider expressed an intention to "audit, inspect, and monitor its subscribers emails," that might be enough to render an expectation of privacy unreasonable.[82] The Justices also recognized that the *Miller* decision may disagree with their findings but noted *Miller* was distinguishable because it involved simple business records rather than "the potentially unlimited variety of confidential communications" at issue in *Warshak*.[83] Although the *Warshak* decision was from a lower court, the opinion offers hope that Fourth Amendment analysis may evolve with emerging technologies.

72. *See id.*

73. *See id.* at 284.

74. *See id.*

75. *See id.*

76. *Warshak*, 631 F.3d at 284.

77. *See id.* at 285–86.

78. *Id.* at 285.

79. *See id.* at 286 (releasing the contents of the emails was ultimately allowed because of the government's good faith reliance on the Stored Communications Act).

80. *See id.* at 286–87.

81. *Warshak*, 631 F.3d at 287–88.

82. *See id.* at 287.

83. *Id.* at 287–88.

B. *United States v. Jones*

United States v. Jones is an example of a case that does not directly involve the application of the third-party doctrine but has the potential to influence this area of the law.[84] In this case, the government installed a GPS tracking device on the defendant's vehicle without a warrant and monitored his movements over the course of four weeks.[85] The Supreme Court found that the government's use of the GPS device to monitor the defendant's movements constituted a search under the Fourth Amendment by applying traditional property principles in the search and seizure analysis.[86] Justice Scalia believed that the actions of the government clearly constituted a physical occupation of "private property for the purpose[s] of obtaining information."[87] Up until the latter half of the twentieth century, Fourth Amendment jurisprudence was tied to common law trespass.[88] The Court chose to once again apply these principles to Fourth Amendment analysis in spite of the growing influence of the *Katz* decision.[89]

The Court struck down the government's contention that the defendant had no reasonable expectation of privacy as to the location of his vehicle on public roads or the underbody of the vehicle where the device was attached because the defendant's rights "do not rise or fall with the *Katz* formulation."[90] The majority felt that, at the very least, they should preserve the degree of privacy against government intrusion "that existed when the Fourth Amendment was adopted."[91] They explained that, for most of our history, the Fourth Amendment has protected us against government intrusion into the areas enumerated and that the *Katz* decision did not revoke this protection.[92] The revitalization of past protections may mark a shift in the way that courts analyze Fourth Amendment claims.

Justice Sotomayor's concurrence is particularly important regarding the third-party doctrine and its application to cases involving emerging technologies.[93] Sotomayor agrees that the physical intrusion is a deciding factor in this case.[94] However, Sotomayor further analyzes the scope of the Fourth

84. *See generally* United States v. Jones, 565 U.S. 400 (2012).

85. *Id.* at 403.

86. *See id.* at 404–05.

87. *Id.* at 404.

88. *Id.* at 405.

89. *See id.* at 406.

90. *Jones*, 565 U.S. at 406.

91. *Id.*

92. *Id.* at 406–07.

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

94. *See id.*

Amendment and its evolving application.[95] Sotomayor particularly conveys her reservations with the application of the third-party doctrine.[96] Her concurrence states "[t]his approach is ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[97]

The concurrence details a number of tasks that Americans participate in daily that may implicate the third-party doctrine but in which most people would not accept the warrantless disclosure of that shared information to the government without complaint.[98] Sotomayor concludes by stating "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."[99] Sotomayor's concurrence has already been widely cited and perhaps reflects a changing attitude in the application of the third party doctrine. This concurrence, coupled with apparently changing attitudes toward the application of property principles, may be the change needed to evolve Fourth Amendment analysis as applied to the increasing number of cases involving emerging technologies.

C. *Riley v. California*

The court in *Riley v. California* determined that the "search incident to arrest" exception does not apply to the digital contents of cell phones.[100] Although the case does not directly implicate the third-party doctrine, the language in the opinion has the potential to strengthen privacy protections surrounding technology in the future. The Court's opinion seems to indicate that the Court is beginning to "engage in the challenges of the digital age ahead."[101] Rather than determine whether there was a reasonable expectation of privacy, the Court analyzed the degree to which the search intruded upon the defendant's privacy and the degree to which such intrusion is needed for

95. *Id.* at 414–18.

96. *Jones*, 565 U.S. at 417.

97. *Id.*

98. *See id.* at 417–18.

99. *Id.* at 418.

100. *See* Riley v. California, 134 S. Ct. 2473 (2014); *see also Fourth Amendment—Search and Seizure—Searching Cell Phones Incident to Arrest—Riley v. California*, 128 HARV. L. REV. 251 (2014) [hereinafter *Fourth Amendment—Search and Seizure*].

101. Marc Rotenberg & Alan Butler, *Symposium: In* Riley v. California*, a Unanimous Supreme Court Sets Out Fourth Amendment for Digital Age*, SCOTUSBLOG (June 26, 2014, 6:07 PM), http://www.scotusblog.com/2014/06/symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amendment-for-digital-age/.

the promotion of legitimate governmental interests.[102] In doing so, the Court listed the qualitative and quantitative differences between cell phones and other objects that are not afforded Fourth Amendment protections.[103]

The unanimous Court noted that the "immense storage capacity" of cell phones and other "digital containers" allows for the collection of many distinct types of information, including data on phones traced back to before the purchase of the device, that are capable of conveying far more than previously possible.[104] They continued by highlighting the sensitivity of the information that can be found in these devices.[105] "A phone not only contains, in digital form, many sensitive records previously found in the home, it also contains a broad array of private information never found in a home in any form."[106] The Court's analysis of stored data, and the Court's ultimate decision, show that the Court is beginning to believe that "files stored in the cloud are deserving of the same (if not more) protection than physical 'papers and effects'" and "that certain types of information are deserving of special protection."[107]

The decision in *Riley* seems to be the Court's way of setting the stage for the battle against the third-party doctrine.[108] The comparison of the qualitative differences of data stored on certain devices shows a shift from the Court's prior distinctions between metadata and content-information.[109] The Court specifically discusses browser history and location information, which, in the past, have been disputed in cases involving warrantless seizure.[110] This analysis in particular may indicate the Court's evolving view on the seizure of "non-content" data.

The conclusion of this opinion is particularly promising for the protection of information stored in our devices and on the cloud.[111]

> The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell

102. *Riley*, 134 S. Ct. at 2478.

103. *See id.* at 2489.

104. *See id.*; *see also Fourth Amendment—Search and Seizure*, *supra* note 100.

105. *Riley*, 134 S. Ct. at 2490.

106. *Id.* at 2491.

107. *See* Rotenberg & Butler, *supra* note 101.

108. *See* Rotenberg & Butler, *supra* note 101.

109. *See Riley*, 134 S. Ct. at 2490.

110. *See id.*

111. *See id.* at 2495.

> phone seized incident to arrest is accordingly simple—get a warrant.[112]

Although the footnotes limit this decision to cases involving searches incident to arrest, it reflects the attitudes of the Justices concerning the protection of digital information.[113] In the future, we may recognize similar language in opinions regarding the application of the Fourth Amendment and the third-party doctrine.

D. *United States v. Graham*

More recently, in *United States v. Graham*, the Fourth Circuit Court of Appeals found that the warrantless procurement of cell-site location information (CSLI) recorded by the defendant's cellular provider was a violation of the Fourth Amendment.[114] Although the decision was later reversed en banc, the decision is still worth discussing when analyzing the evolution of third-party doctrine application to Fourth Amendment claims.[115] In this case, while investigating a string of robberies, the government obtained CSLI from the defendant's cellular provider for a 221-day time period.[116] CSLI allows the government to identify the location around which a cellular device was located at a given time by identifying the cell sites from which a cell phone has sent or received radio signals.[117] The court, in its initial decision, found that the "government conducts a search under the Fourth Amendment when it obtains and inspects a cell phone user's historical CSLI for an extended period of time."[118]

"Considering the multiple privacy interests at stake," the court recognized that a cell phone user has a reasonable "expectation of privacy in their long-term CSLI."[119] Additionally, the court rejected the argument that the carrier's privacy policy showed there was no expectation of privacy in their CSLI because the policy stated the carrier "*collects* information about the phone's location—not that it discloses this information" to others.[120] The

112. *Id.*

113. *See id.* at 2489, n.1 ("Because the United States and California agree that these cases involve *searches* incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.").

114. *See* United States v. Graham, 796 F.3d 332 (4th Cir. 2015) (adhered to in part on reh'g en banc, 824 F.3d 421 (4th Cir. 2016)).

115. *See* United States v. Graham, 824 F.3d 421 (4th Cir. 2016).

116. *See Graham*, 796 F.3d at 341.

117. *See id.* at 343.

118. *Id.* at 344–45.

119. *Id.* at 349.

120. *Id.* at 345.

court also highlights the fact that most users do not even read, much less understand, the carrier's privacy policy.[121] Finally, the court specified that the third-party doctrine does not apply to CSLI because users do not *voluntarily* convey location information to carriers[122] and because CSLI is more sensitive than noncontent information.[123] Notably, Judge Motz dissented in part, concluding that the defendants voluntarily shared their CSLI with third parties and therefore there was no reasonable expectation of privacy in it.[124] On rehearing en banc, Motz is in the majority and expounds on her dissent in the decision that carries the day.[125]

Writing for the majority, Motz begins by stating that defendants have no reasonable expectation of privacy in information that is voluntarily handed over to a third party, even if that information is revealed under the assumption that it would be used for a limited purpose.[126] The majority believes that the defendant, and, by implication, the majority in the previous hearing, disregarded precedent, "misunderst[ood] the nature of CSLI, improperly attempt[ed] to redefine the third-party doctrine, and blur[red] the critical distinction between content and non-content information."[127]

However, the majority never discussed the subjective and objective elements of the *Katz* test to determine whether there was actually a reasonable expectation of privacy.[128] The *Graham* court simply assumes that there is no reasonable expectation of privacy because the information was "voluntarily" conveyed to a third party.[129] In the precedent cited, the fact that the information was voluntarily conveyed to a third party was the beginning of the court's analysis, not the end.[130] Although the court in *Graham* makes their

121. *Id.*

122. *Graham*, 796 F.3d at 353.

123. *See id.* at 358–59.

124. *See id.* at 378–80.

125. *See* United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc).

126. *Id.* at 425.

127. *Id.*

128. *See id.* at 421.

129. *See id.*; *see also Fourth Amendment—Third-Party Doctrine—Fourth Circuit Holds That Government Acquisition of Historical Cell-Site Location Information is Not a Search*, 130 HARV. L. REV. 1273, 1277 [hereinafter *Fourth Amendment—Third-Party Doctrine*] ("But *Graham* shows that courts have shifted from trying to estimate what society really would consider reasonable, as they did in the cases establishing the third-party doctrine, to substituting a doctrinally constructed determination of reasonableness through the third-party doctrine.").

130. *See* Smith v. Maryland, 442 U.S. 735, 735 (1979); *see also* United States v. Miller, 425 U.S. 435, 435 (1976)

decision based on precedent, it seems that prior decisions may have been misapplied.[131]

Although citing Supreme Court precedent as the reason for the reversal en banc, Motz states that "[t]he Supreme Court may in the future limit, or even eliminate, the third-party doctrine. Congress may act to require a warrant for CSLI. But without change in controlling law, we cannot conclude that the Government violated the Fourth Amendment in this case."[132] The Supreme Court may have its chance. A case with a strikingly similar fact pattern was heard by the Court in November 2017, and their decision should be released around June of 2018.[133]

In *Carpenter v. United States*, the Supreme Court must decide whether the warrantless collection of CSLI over a 127-day period violates the Fourth Amendment.[134] The president of the National Constitution Center, a nonprofit devoted to educating the public about the Constitution, believes that this could be the "most important electronic privacy case of the 21st century."[135] Apple, Facebook, and Google, among other technology companies, filed a brief that urged the Court to modernize the Fourth Amendment.[136] The brief said that "[n]o constitutional doctrine should presume [. . .] that consumers assume the risk of warrantless government surveillance simply by using technologies that are beneficial and increasingly integrated into modern life."[137] It is impossible to determine how the Court is going to decide, but the outcome could transform Fourth Amendment law. The government argues that the third-party doctrine applies.[138] Carpenter argues that he has a reasonable expectation of privacy in his CSLI.[139] In oral arguments, Justice Gorsuch wanted to focus on a property-based approach to analyzing the war-

131. *See Graham*, 824 F.3d at 425.

132. *Id.*

133. *See* Ariane de Vogue, *Supreme Court Takes on Major Fourth Amendment Case*, CNN (Nov. 29, 2017), http://www.cnn.com/2017/11/29/politics/supreme-court-fourth-amendment-case/index.html.

134. *See* Adam Liptak, *How a Radio Shack Robbery Could Spur a New Era in Digital Privacy*, N.Y. TIMES (Nov. 27, 2017), https://www.nytimes.com/2017/11/27/us/politics/supreme-court-fourth-amendment-privacy-cellphones.html.

135. *Id.*

136. *Id.*

137. *Id.*

138. *See* Mark Joseph Stern, *Neil Gorsuch's Independent Streak*, SLATE (Nov. 30, 2017), http://www.slate.com/articles/news_and_politics/jurisprudence/2017/11/in_carpenter_v_united_states_neil_gorsuch_showed_his_independent_streak.html.

139. *See id.*

rantless acquisition of stored data.[140] No matter the decision, the Fourth Amendment and the third-party doctrine will be affected.

IV. VIRTUAL ASSISTANTS

We should briefly discuss what exactly a virtual assistant (i.e. Amazon Echo) is and how it may present problems in third-party doctrine cases before considering a solution to the application of the Fourth Amendment to emerging technologies. Virtual assistants can be found in many devices and are offered by several tech companies.[141] These voice-activated assistants can perform a variety of tasks: playing music, turning your lights on, adjusting the thermostat, or locking your doors.[142] Virtual assistants are being integrated into a number of third-party devices, including vehicles.[143] It is safe to say that tech companies are striving to make these platforms indispensable and omnipresent.[144] Thirty-nine million Americans own a smart speaker that features a virtual assistant.[145] As of January 2017, nearly 77% of Americans owned a smartphone, and many of those devices featured virtual assistants.[146]

So why are these devices so important in the Fourth Amendment context? Virtual assistants, such as the Amazon Echo and Google Home, record voice commands and send them to the manufacturer's data center.[147] Devices such as these only record when they hear their "wake words," like "hey Alexa" or "hey Google."[148] Once the device hears the "wake word," it begins recording, it transmits the data to the manufacturer, the data is processed, and then a response is transmitted back to the device.[149] What users might not

140. *See id.*

141. *See* Jon Martindale, *Cortana vs. Siri vs. Google Assistant*, DIGITAL TRENDS (Aug. 12, 2018), https://www.digitaltrends.com/computing/cortana-vs-siri-vs-google-now/.

142. *See* Kim Wetzel, *What is Alexa? It's Amazon's Virtual Voice Assistant*, DIGITAL TRENDS (May 11, 2018, 11:09 AM), https://www.digitaltrends.com/home/what-is-amazons-alexa-and-what-can-it-do/.

143. *See* Daisuke Wakabayashi & Nick Wingfield, *Alexa, We're Still Trying to Figure Out What to Do With You*, N.Y. TIMES (Jan. 15, 2018), https://www.nytimes.com/2018/01/15/technology/virtual-assistants-alexa.html.

144. *See id.*

145. *See* Browne, *supra* note 4.

146. *See* Aaron Smith, *Record Shares of Americans Now Own Smartphones, Have Home Broadband*, PEW RES. INST. (Jan. 12, 2017), http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/.

147. *See* Deanna Paul, *How Smart Devices Could Violate Your Privacy*, ROLLING STONE (July 24, 2017), https://www.rollingstone.com/culture/features/how-smart-devices-could-violate-your-privacy-w492823.

148. *See id.*

149. *See id.*

know about this process is that the manufacturer actually records and stores all of the audio just before and following the "wake word," or even words that sounds similar to the wake word.[150] For instance, if a virtual assistant user is having a conversation with a confidant in a room near an Alexa device and says something along the lines of "I killed Alex. How do we get rid of the body?" Amazon has that audio stored on their servers, and the government may have access to that information without a warrant. The user wasn't voluntarily conveying that information to the device, but the device recorded the information anyway. How would the Court analyze a Fourth Amendment claim in this, or a similar, situation?

The previous scenario may seem far-fetched, but cases like these have already been considered in the United States.[151] In November 2015, the authorities in Bentonville, Arkansas found a body floating in a hot tub.[152] The homeowner told the police that he was in bed and that the victim stayed up drinking.[153] The suspect (the homeowner) had an Alexa powered device in his home, and the authorities subpoenaed Amazon to recover the recordings that were stored from the suspect's virtual assistant.[154] Fortunately for the suspect, Amazon refused to turn over the information citing First Amendment protections, but you can imagine a scenario in which Amazon turned over the data, and then a Fourth Amendment claim is born.[155] The virtual assistant is just one of the many emerging technologies that will require the Fourth Amendment to evolve in order to provide adequate privacy protections. As much as we rely on these technologies, it would not be unreasonable for the Court to find that users have a reasonable expectation of privacy in the data shared with third parties through these devices and that society is prepared to recognize this expectation as reasonable.

V. HOW DO WE FIX IT? THE APPLICATION OF THE THIRD-PARTY DOCTRINE

The court in *Riley v. California* spoke on the issues surrounding the application of the Fourth Amendment to current technologies: "In light of these developments, it would be very unfortunate if privacy protection in the 21st century was left primarily to the federal courts using the blunt instru-

150. *See id.*; *see also* Brian Heater, *Can Your Smart Home Be Used Against You in Court?*, TECH CRUNCH (Mar. 12, 2017), https://techcrunch.com/2017/03/12/alexa-privacy/.

151. *See* Gerald Sauer, *A Murder Case Tests Alexa's Devotion to Your Privacy*, WIRED.COM (Feb. 28, 2017), https://www.wired.com/2017/02/murder-case-tests-alexas-devotion-privacy/; *see also* Heater, *supra* note 150.

152. *See* Heater, *supra* note 150.

153. *See* Heater, *supra* note 150.

154. *See* Sauer, *supra* note 151; *see also* Heater, *supra* note 150.

155. *See* Sauer, *supra* note 151; *see also* Heater, *supra* note 150.

ment of the Fourth Amendment. Legislatures, elected by the people, are in a better position to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future."[156] Absent sweeping legislation, which would be nearly impossible to pass in this political climate, the Court must find a way to balance the expectation of privacy against enforcement of the law in a way that does not discourage innovation or the adoption of new technologies.

The Court can solve this problem by getting back to weighing the facts specific to the case against the test formulated in the *Katz* concurrence rather than simply deciding that there is no reasonable expectation of privacy when information is voluntarily conveyed to a third party.[157] This will require not only that the two-prong test be applied, but also that the Court examine the definition of "voluntary" and reevaluate what constitutes the "sensitivity of information" conveyed when determining whether there is a subjective expectation of privacy.

It seems that courts have moved away from applying the two-part test and towards a simple determination of whether the party could expect privacy; however, in order for any of the new interpretations to matter, the Court must apply the facts to the two-part *Katz* test. Most recently in *Graham*, the court simply assumes there is no reasonable expectation of privacy because the information was "voluntarily" conveyed to a third party.[158] The Court must get back to applying the two-part *Katz* test in third-party doctrine cases and must further evolve its interpretations of the factors involved along with the evolution of our dependence on technology.

Again, the *Katz* formula requires that the Court examine whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy."[159] The majority believed that this is met when "the individual has shown that he seeks to preserve [something] as private."[160] Then, the Court must determine whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as reasonable."[161] The *Katz* majority believed this meant whether the individual's expectation, viewed objectively, is "justifiable" under the circumstances.[162] When applied to the facts in *Smith*, the Court rejected the idea that the petitioner had a legitimate

156. Riley v. California, 134 S. Ct. 2473, 2497–98 (2014).

157. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also* Smith v. Maryland, 442 U.S. 735, 744–45 (1979).

158. *See* United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) (en banc); *see also Fourth Amendment—Third-Party Doctrine*, *supra* note 129, at 1277.

159. *Katz*, 389 U.S. at 361.

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

161. *Id.* at 361 (Harlan, J., concurring).

162. *Smith*, 442 U.S. at 740.

expectation of privacy regarding the numbers he dialed on his phone.[163] The Court seemed to imply that the test only applies when the information obtained does not consist of "content" information.[164] The Court then rejected petitioner's claim that he had a reasonable expectation of privacy in the numbers he dialed because they "doubt that people in general entertain any actual expectation of privacy in the numbers they dial."[165] The majority also focused on the fact that the numbers are "conveyed" to the telephone company and the company has the ability to maintain records, as phone companies generally do, for "a variety of legitimate business purposes."[166] The Court also rejected the petitioner's argument that his conduct, using the phone in his own home to the exclusion of all others, demonstrated a reasonable expectation of privacy.[167] "Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed."[168]

The Court doubled down and opined that even if petitioner had a reasonable expectation of privacy, that expectation was not "one that society was ready to recognize as reasonable."[169] The majority believed this to be so because the petitioner "voluntarily" conveyed the information to a third party.[170] The Court cited *Miller* when determining that, because the information was voluntarily conveyed to a third party, the petitioner assumed the risk that the information would be divulged to the police.[171]

A. Follow *Smith* and *Miller*: Get Back to the *Katz* Test

The latest trend in third-party doctrine cases is simply the recitation of precedent, deciding that there is no reasonable expectation of privacy in information because it was voluntarily conveyed to a third party rather than applying the *Katz* test.[172] When determining whether there is a reasonable expectation of privacy, the Court in *Miller* and *Smith*, the oft cited precedent,

163. *See id.* at 741.

164. *See id.* at 742 ("Given a pen register's limited capabilities, therefore, 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.").

165. *Id.*

166. *See id.* at 743.

167. *Id.*

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

169. *Id.* at 743–44 (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

170. *See id.*

171. *Id.* at 744.

172. United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016).

applied a two-part test, and the fact that information was voluntarily conveyed to a third party was simply one of many factors considered in finding no reasonable expectation of privacy.[173] In order to ensure that privacy interests are being protected, the Court must get back to applying the *Katz* test and consider the totality of the circumstances before deciding there is no reasonable expectation of privacy.

B. Conduct of the Individual: Presumption of Privacy Inside a Home

When applying the *Katz* test to cases that implicate the third-party doctrine, there are many factors that have been used in the Court's analysis.[174] The *Katz* majority believed that the subjective element would be met if the individual showed "he seeks to preserve [something] as private."[175] The Court should not only consider the actions of an individual, such as closing the door of a phone booth behind them,[176] but should also consider where these actions take place. "Doctrinally, homes receive greater protection than many contexts of search and seizure; only a few contexts, such as telephone booths and bodily invasion, receive greater protection."[177] The Fourth Amendment itself:

> [E]mbodies a spiritual concept: the belief that to value the privacy of *home* and person and to afford it constitutional protection against the long reach of the government is no less than to value human dignity, and that this privacy must not be disturbed except in case of overriding social need, and then only under stringent procedural safeguards.[178]

A number of Supreme Court cases have recognized the sanctity of the home and the protection afforded by the Fourth Amendment.[179] The dissent

173. *See* United States v. Miller, 425 U.S. 435, 442–47 (1976); *see also Smith*, 442 U.S. at 740–46.

174. *Id.*

175. *Katz*, 389 U.S. at 351.

176. *See id.* at 361 (Harlan, J., concurring).

177. Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905, 912 (2010).

178. Commonwealth v. Livingstone, 174 A.3d 609, 642 n.2 (Pa. 2017) (citing JACOB W. LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT 47 (1966)).

179. *See* United States v. Karo, 468 U.S. 705, 714 (1984) ("[P]rivate residences are places in which the individual normally expects privacy . . . and that expectation is plainly one that society is prepared to recognize as justifiable."); *see also* Groh v. Ramirez, 540 U.S. 551, 559 (2004) (holding that warrantless searches and seizures inside a home are "presumptively unreasonable").

in *Smith* seems to agree that the home is sacred.[180] "The information captured by such surveillance emanates from private conduct within a person's home or office-locations that without question are entitled to Fourth and Fourteenth Amendment protection."[181] When analyzing whether there is a subjective expectation of privacy, the location of the action should be considered. There should be a presumption of a reasonable expectation of privacy in actions taken at home. For example, the Court in *Smith* should have considered that the petitioner made the phone calls from the comfort of his own home without broadcasting the numbers to the outside world as the dissent seems to do.[182] This should not be a deciding factor, but it most certainly should hold some weight that must be overcome by other circumstances for the Court to decline to recognize a reasonable expectation of privacy.

C. What is "Voluntary?"

Another significant factor in the Court's determination of whether there is a reasonable expectation of privacy that society is prepared to recognize as reasonable is the voluntary nature of the conveyance of the information.[183] The Supreme Court makes this clear by stating:

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[184]

In *Miller*, the Court found that the petitioner had no reasonable expectation of privacy in bank records that were "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business" and then provided to the government.[185] In *Smith*, the court found no reasonable expectation of privacy "when petitioner voluntarily conveyed numerical information to the phone company and 'exposed' that information to its

180. *See* Smith v. Maryland, 442 U.S. 735, 747 (1979) (Stewart, J., dissenting).

181. *Id.*

182. *See id.*

183. *See id.* at 743–44 (majority opinion) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); *see also* United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) ("For the Court has long held that an individual enjoys no Fourth Amendment protection 'in information he voluntarily turns over to a third party.'").

184. United States v. Miller, 425 U.S. 435, 443 (1976).

185. *Id.* at 442.

equipment in the normal course of business."[186] Both of the dissents in these cases, as well as many other third-party doctrine cases, questioned the "voluntary" nature of these conveyances.[187] It is time for the Court to recognize that much of what we convey to third parties today is not truly "voluntary" in nature.

More recently, in *United States v. Jones*, Justice Sotomayor discussed the prevalence with which we share information with others today.[188] She believes that the Court's approach in denying to find a reasonable expectation of privacy is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[189] The Court must follow suit and reevaluate what they consider to be "voluntary." Under the current interpretation of the third-party doctrine, to avoid the reach of the government, an individual would have to refrain from storing their money in banks and make all payments using cash. All communications would have to be made in person or via carrier pigeon.

These actions are unrealistic in a world full of technology that could not even have been imagined when the *Katz* or *Miller* opinions were being written. The definition of "voluntary" must evolve with technology and its adoption by America's citizens. An individual's transactional records with a bank are not "voluntarily" conveyed. "It is impossible to participate in the economic life of contemporary society without maintaining a bank account."[190] An individual's cell-site location data is not truly "voluntarily" conveyed. "There is no reason to think that a cell phone user is aware of his CSLI, or that he is conveying it. He does not write it down on a piece of paper . . . or enter it into a device."[191] Cellular providers can simply track the area in which a cellular device is located at a given time because its customer carries the phone with them at all times.[192] With the need to be connected at all times, nine-in-ten cellphone owners say they "frequently" carry their phones

186. *Smith*, 442 U.S. at 735.

187. *See Miller*, 425 U.S. at 451 (Brennan, J., dissenting) ("For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."); *see also Smith*, 442 U.S. at 750 (Marshall, J., dissenting).

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

189. *Id.*

190. *Miller*, 425 U.S. at 451 (Brennan, J., dissenting).

191. United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) (Wynn, J., dissenting).

192. *See* United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016).

with them.[193] Is ownership of a cellular phone truly "voluntary" in nature? It could be argued that an individual *must* own a cell phone to function in today's society.

Black's Law Dictionary defines "voluntary" as "done by design or intention; unconstrained by interference; not impelled by outside influence; having merely nominal consideration."[194] Cell phone ownership and bank accounts, for instance, are intentional acquisitions, but are they impelled by outside influence? Does society require that one own a cellular phone or have a bank account? Many would argue that these are necessary to be a contributing member of society. The Court must take a closer look at what "voluntary" truly means when analyzing a third-party doctrine case.

D. Sensitivity of Information

Finally, the Court analyzes the sensitivity of the information conveyed when coming to the conclusion that an individual has no reasonable expectation of privacy in the information conveyed to third parties.[195] The Court in *Miller* examined "the nature of the particular documents sought to be protected in order to determine whether there [was] a legitimate 'expectation of privacy' " concerning the contents of petitioner's bank records.[196] If the subpoena sought the contents of the customer's safe deposit box, would the outcome have been different? What makes bank records less sensitive than cash and jewelry in a safe deposit box? It can be argued, for instance, that bank records tell authorities much more about an individual than security footage from the bank. The Court in *Smith* determined that the numbers dialed from a phone are not sensitive enough to warrant a reasonable expectation of privacy.[197] In the dissent, Justice Stewart opined that "the numbers dialed from a private telephone—although certainly more prosaic than the conversation itself—are not without content . . . because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[198]

The Court should dig deeper into the sensitivity of the information conveyed rather than simply deciding that they "doubt that people in general entertain any actual expectation of privacy in the numbers they dial," for

193. *See* Lee Rainie & Kathryn Zickuhr, *Americans' Views on Mobile Etiquette*, Pew Res. Ctr. (Aug. 26, 2015), http://www.pewinternet.org/2015/08/26/chapter-1-always-on-connectivity/.

194. *Voluntary*, Black's Law Dictionary (10th ed. 2014).

195. *See Miller*, 425 U.S. at 442–43; *see also* Couch v. United States, 409 U.S. 322, 335–36 (1973).

196. *See Miller*, 425 U.S. at 442–43.

197. *See* Smith v. Maryland, 442 U.S. 735, 743 (1979).

198. *Id.* at 748 (Stewart, J., dissenting).

instance.[199] The Court's reasoning for making decisions such as this is because users "realize that they must 'convey'" information to various companies so these companies may complete their transactions.[200] Telephone users must convey phone numbers to the telephone company since it is through the telephone company switching equipment that their calls are completed: does that sound voluntary?[201] Individuals are not implying that the information that they *must* share is not sensitive simply by conveying this information to a third party. The Court must move back to a context-based approach when determining whether there is a reasonable expectation of privacy in information shared with a third party.

VI. POSSIBLE PROBLEMS WITH PROPOSED SOLUTION

The proposed solution is not without problems. In the most recent decisions, such as *Graham*, courts have failed to even apply the *Katz* test. The Court would have to overrule prior decisions by deciding that voluntarily conveying information to a third party is not a determinative factor in third-party doctrine cases. However, the Supreme Court would be moving back to the application of *Smith* and *Miller*, older precedent, and applying these cases and their reasoning moving forward rather than applying their new decisions retroactively.

An additional problem with the proposed solutions discussed may cause the Court to draw arbitrary lines in determining what is voluntary, what is sensitive, and what conduct is to be considered worthy of an expression of a subjective expectation of privacy. However, it seems that Courts have already drawn arbitrary lines when determining what warrants a reasonable expectation of privacy. For instance, the Court in *Smith* decided that the phone numbers and individual dials are not "sensitive" in nature.[202] Furthermore, the in-depth analysis proposed could be a burdensome task on the Court. If the Court must apply each fact pattern and analyze it under the *Katz* test rather than simply deciding there is no reasonable expectation of privacy because an individual shared information with a third party, the Court may find itself accepting many more cases that implicate the third-party doctrine before establishing a new line of precedent. In addition, new technologies emerge every day, and, without a blanket decision, new issues will arise that will produce litigation.

However, the interest in privacy outweighs judicial economy. Establishing a line of precedent that balances an interest in privacy with an interest in law enforcement that is relevant to the technological world in which we live is worth the additional work that would be necessary to update third-party doctrine application. If the *Graham* decision is an indication of what is to

199. *Id.* at 742 (majority opinion).

200. *See id.*

201. *Id.*

202. *See Smith*, 442 U.S. at 742.

come, then nearly all of our information the Court finds to be "non-sensitive" will be available to the government without a warrant. We share nearly everything with a third party in society today, and we must protect this information without placing an undue burden on law enforcement.

VII. IMPLICATIONS OF THE USE OF VIRTUAL ASSISTANTS

Under current judicial interpretations, if the Court were to subpoena the data from a smart device with a virtual assistant, the Court may find that the user has no reasonable expectation of privacy in "non-content" information but would protect the actual audio recorded. It is difficult, to be sure, because this particular scenario has yet to play out in the courts. Consider a hypothetical case in which the defendant was suspected of a murder. In the defendant's home, he had an Amazon Echo device. The authorities subpoena Amazon to obtain the information shared with them by the defendant. Under the current interpretation of the third-party doctrine, the information would be allowed to convict the defendant as long as it did not contain the actual audio. Some examples of information that may be allowed include purchase information, scheduled appointments, location information, and web searches, all without a warrant. Under the proposed solutions, when analyzing the defendant's claim that an unlawful search occurred when the government obtained this data without a warrant, the courts would begin by applying the *Katz* test. First, did the petitioner exhibit an actual expectation of privacy?[203] Second, is that expectation one that society is prepared to recognize as reasonable?[204]

The Court in *Smith* and *Miller* consider the sensitivity of the information conveyed and the circumstances surrounding the conveyance when determining whether the individual has shown that he seeks to preserve something as private.[205] Under the proposed solution, the Court would start by presuming a privacy interest in this information, because the petitioner's interactions with his virtual assistant via his Echo device took place in the home. It is clear that the petitioner wished for these interactions to remain private because he could have left his home and made the hypothetical purchases rather than asking Alexa. He could have ventured to the library and researched "how to dispose of a body" rather than asking Alexa. He believed that, in the safety of his own home, his information would remain private. To overcome the presumption, the Court could then weigh the sensitivity of the information and the defendant's other actions against the presumption of privacy.

When analyzing the sensitivity of the information, the Court should not simply decide that no reasonable person believes that his web searches and purchase information are protected. The Court should dig in to what informa-

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

204. *Id.*

205. *See* United States v. Miller, 425 U.S. 435, 442–47 (1976); *see also Smith*, 442 U.S. at 740–46.

tion the government can glean from something that seems as "harmless" as the numbers dialed on a phone.[206] Purchase information not only contains groceries and clothing but also a number of other things that individuals may wish to keep private, such as medication or items that could be embarrassing or harmful to one's reputation. An individual's search history produces the same conclusions, as evidenced by "If I die, delete my browser history" t-shirts that can be purchased today. In this case, the sensitivity of the information conveyed would not give the Court an adequate reason to overcome the presumption that the petitioner sought to keep the information conveyed from his home private and, therefore, had a subjective reasonable expectation of privacy.

The Court would then analyze whether the expectation is one that society is prepared to recognize as reasonable.[207] The Courts in *Smith* and *Miller* seem to determine that society is not prepared to recognize an expectation as reasonable when an individual *voluntarily* turns information over to third parties.[208] Under the proposed solution, the Court would analyze the voluntary nature of the conveyance. *Black's Law Dictionary*'s definition of voluntary includes "not impelled by outside influence."[209] The Court would have to determine if societal norms are considered an "outside influence." The regularity with which we use technology to make our purchases and do our research, among other things, and, as a result, share our information with a third party, seems to indicate that these actions are not truly voluntary, but more of a necessity.[210]

It is true that an individual chooses to make a purchase through a virtual assistant "voluntarily" within the simplest meaning of the word, but to say that an individual is "voluntarily" sharing that purchasing information with a third party is a stretch. An alternative to making a purchase through a smart device would be to go to the store and make the purchase at the physical location. But at the store, you are "sharing" your purchase information with the teller and even your bank when you use a debit or credit card. Sharing purchase information with a third party is absolutely necessary in order to participate in a transaction, and, thus, is not truly voluntary. The analysis is the same for search histories. By digging deeper into the analysis of whether information is "voluntarily" conveyed, the Court should determine that this information is not, in fact, voluntarily shared, and thus should come to the

206. *See Smith*, 442 U.S. at 748 (Stewart, J., dissenting) ("I doubt there are any who would be happy to have broadcast to the world a list of the . . . numbers they have called . . . because it easily could reveal the identities of the persons and the places he called, and thus reveal the most intimate details of a person's life.").

207. *See id.* at 743–44 (majority opinion).

208. *See id.*; *see also Miller*, 425 U.S. at 442.

209. *Voluntary*, BLACK'S LAW DICTIONARY (10th ed. 2014).

210. *See* Browne, *supra* note 4.

determination that there is a reasonable expectation of privacy in this information.

Although under this hypothetical, the government would not be able to use this information against the defendant because it was obtained without a warrant, the government could avoid this scenario altogether if they receive a warrant prior to the collection of the information. This solution does not hinder law enforcement to the extent that they will not be able to convict criminals. It simply ensures that law enforcement obtains information in a way that allows for consideration of the suspect's Fourth Amendment privacy interests beforehand. The warrant requirement in the Fourth Amendment was included for this very reason.[211]

VIII. CONCLUSION

The current interpretation of the third-party doctrine is in danger of completely nullifying Fourth Amendment protections in a world that all but requires us to share our information with third parties. The trend of disregarding the test set forth in *Katz* and replacing it with the determination that whatever information is "voluntarily" conveyed to a third party is afforded no Fourth Amendment protection is a misapplication of precedent. The Court must get back to applying the *Katz* test in third-party doctrine analysis.

However, the application of the *Katz* test consistent with *Smith* and *Miller* is a merely a half-baked solution. The Court should go one step further in analyzing the factors and propose a presumption of privacy in actions taken in the home. In addition, the Court's definition of "voluntary" should be reexamined, and the decision that information lacks sensitivity should require further analysis. Without change, the government has warrantless access to a wealth of information that most citizens would consider private. In the words of Justice Sotomayor, the current approach "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[212] The Court should heed her words and make a change before the Fourth Amendment vanishes in the wake of technological advancements.

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

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