Missouri Law Review

Volume 83
Issue 4 *Fall 2018 - Symposium*

Article 10

Fall 2018

Technology or Privacy: Should You Really Have to Choose Only One?

Callie Haslag

NOTE

Technology or Privacy: Should You Really Have to Choose Only One?

Callie Haslag[*]

I. INTRODUCTION

Today's society has both the blessing and the curse of having access to a vast range of technologies. A person can be diagnosed by doctors while video-chatting from his or her own home, communicate with someone located on the other side of the world instantaneously, or monitor his or her home through enhanced security systems. It is even possible to give simple commands, like "Turn on the lights" or "Play my favorite song," and a home assistant device, such as the Amazon Echo, will complete the given task. While these technologies offer many blessings, there are potential downsides that accompany their presence.

People are currently living in the Information Age, where devices record and collect data based on their personal information.[1] This data is often stored by third parties, including, but not limited to, internet service providers, phone companies, websites, and merchants.[2] This data is used for different purposes, but most is used for advertising and learning a user's preferences.[3] However, this information can also be made available to the government – specifically for law enforcement's use.[4] The data collected by these third parties provides detailed records as to an "individual's reading materials, purchases, diseases, and website activity," which "enable[s] the government to assemble a profile of an individual's finances, health, psychology, beliefs, politics, interests, and lifestyle."[5] Therefore, the government could know more about a person than even his or her closest family members and friends.

One of the latest technologies taking hold across America is the smart home device. These devices include products such as Amazon's Echo, Nest's connected home devices, smart water meters, and

---

[*] B.S., Political Science and Economics, Minor in Business from the University of Missouri; J.D. Candidate, University of Missouri School of Law, 2019; Associate Member, *Missouri Law Review*, 2017-2018. I am grateful to Professor Desnoyer for his insight, guidance, and support during the writing of this Note, as well as the *Missouri Law Review* for its help in the editing process.

1. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002).
2. *Id.* at 1084.
3. *See id.* at 1141–42.
4. *Id.*
5. *Id.* at 1084.

even refrigerators with interior cameras that broadcast directly to a person's phone. These devices monitor and record data from users' homes, which is then stored by the third parties providing the services.[6] This data, while appearing to be under a user's sole control, can be used by the third-party service provider.[7] Law enforcement agencies seek to access the data held by third-party service providers to collect private information about individuals when investigating crimes like drug trafficking, white-collar offenses, cyber misconduct, and even more serious crimes, like murder.[8]

For example, in November of 2015, law enforcement requested that Amazon turn over data it collected from an Amazon Echo, which was located in a home where a death occurred.[9] Amazon refused.[10] Despite the fact that the police secured a search warrant, Amazon refused the request on privacy grounds, stating it would not release customer information "without a valid and binding legal demand properly served."[11] Amazon also objected to what it felt were "overbroad or otherwise inappropriate demands."[12] Eventually, Amazon turned over the data; however, it did so only after the Echo owner, and suspected murderer, gave consent.[13] As there are currently few standards for how smart home devices should be treated under the law, this Note explores existing case law to assess and articulate how the government should treat the data these devices collect.

II. LEGAL BACKGROUND

There are two main areas of law surrounding the issue of privacy and technology: privacy law and the third-party doctrine.

A. The Fourth Amendment and Early Privacy Law

Privacy law is complicated because it must evolve to address ever-changing technology to protect the fundamental rights that have existed since our nation's founding. Protecting one's personal information was significantly easier prior to the invention of telephones, GPS, and the Internet. However, it

6. Keith Allen & Eliott C. McLaughlin, *Alexa, Can You Help with This Murder Case?*, CNN (Dec. 28, 2016, 8:48 PM), http://www.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/index.html.

7. *See id.*

8. *See* Solove, *supra* note 1, at 1084.

9. Allen & McLaughlin, *supra* note 6.

10. *Id.* The suspect had held a get together at his home, which involved alcohol. *Id.* The next morning, a guest was found floating face-down in the hot tub, and the deceased's blood alcohol content was four times the legal driving limit. *Id.* Investigators believed there were signs pointing to foul play, so they sought the data from the Amazon Echo in hopes to gather more information to solve the case. *Id.*

11. *Id.*

12. *Id.*

13. *See id.*

is still just as important now as it was prior to these technological advancements to protect a person's right to privacy. To fully understand privacy law today, one must possess a background understanding of how it has evolved.

1. Pre-*Olmstead* Privacy Law

The Fourth Amendment provides the first major source for protecting privacy from law enforcement infringement. The Fourth Amendment secures Americans' right to "be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[14] It further requires probable cause for warrants.[15] This Amendment was intended to guarantee the "privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the government."[16] In its jurisprudence, the United States Supreme Court has defined "search" as a government infringement upon "an expectation of privacy that society is prepared to consider reasonable."[17] Additionally, the Court has defined a "seizure" of property as "some meaningful interference with an individual's possessory interests in that property."[18] Therefore, as a general matter, warrantless searches are "per se unreasonable under the Fourth Amendment," although there are a "few specifically established and well-delineated exceptions."[19] "[T]he Fourth Amendment concerns itself with 'informational security' arising from 'constitutional sources . . . . 'Informational security' [refers to] personal information that is secured in some manner from governmental intrusion . . . . '[C]onstitutional sources' means the textually referenced, 'persons, houses, papers, and effects.'"[20]

To implicate the Fourth Amendment, a government agent must conduct a "search" or "seizure."[21] The first Fourth Amendment case relevant to this topic was *Boyd v. United States*,[22] which involved a court order demanding a commercial glass company to produce its private business papers.[23] The Court held that the order violated the Fourth Amendment because such a demand was an "invasion[] on the part of the government . . . of the sanctity of a man's home

14. U.S. CONST. amend. IV.

15. *Id.*

16. City of Ontario v. Quon, 560 U.S. 746, 755–56 (2010).

17. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

18. *Id.*

19. Katz v. United States, 389 U.S. 347, 357 (1967); *see also* Riley v. California, 134 S. Ct. 2473, 2483 (2014) (discussing the search of a suspect based on probable cause and incident to a lawful custodial arrest as such an exception); O'Connor v. Ortega, 480 U.S. 709, 725 (1987) (holding that the "special needs" of the workplace justify one such exception).

20. Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 604 (2017).

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

22. 116 U.S. 616 (1886).

23. *Id.* at 617–18.

and the privacies of life."[24] The Court further articulated that it was "not the breaking of his doors, and the rummaging of his drawers, that constitute[d] the essence of the offen[s]e[] but [rather] *the invasion of [the] indefeasible right of personal security, personal liberty and private property,* where that right [had] never been forfeited by [a] conviction of some public offense . . . ."[25]

The Court in *Boyd* was not focused on a physical harm but rather the harm of revealing information.[26] Additionally, the focus was not on the company's papers themselves but rather on the content contained *in* the papers.[27] Further, the Court distinguished business records from personal records, such as a diary.[28] The reach of these "privacies of life" go beyond personal information and cover "privately held, but not overtly intimate[,] information."[29] "[T]his broad protection . . . was [later] replaced with a more limited, physically-oriented, property-based" framework.[30]

2. *Olmstead v. United States*[31]

Although it is hard to imagine life without the various forms of technology that influence people each day, the world was not always so technologically advanced. There was a time when the telephone was considered a major technological advancement. Even then, telephone users learned that private telephone calls could be affected by the surveillance of third-party service providers and law enforcement.[32]

The first major decision regarding surveillance technology was *Olmstead v. United States*,[33] where the Court held there is no reasonable expectation of privacy in telephone calls when no physical trespass occurs; moreover, the Court allowed the warrantless tapping of phone lines.[34] In *Olmstead*, federal

---

24. *Id.* at 630.

25. *Id.* (alteration in original).

26. Ferguson, *supra* note 20, at 569.

27. *Id.*

28. *Id.*

29. *Id.*

30. *Id.*

31. 277 U.S. 438 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

32. Wiretapping predates the invention of the telephone. April White, *A Brief History of Surveillance in America*, SMITHSONIAN.COM (Apr. 2018), https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/. The first statute prohibiting wiretapping regarded telegraph lines. *Id.* Prior to the Prohibition, this form of ease-dropping was predominately used by private detectives and corporation. *Id.* After the Prohibition hit, law enforcement utilized wiretapping, and the Court in 1928 "narrowly affirmed the constitutionality of police wiretapping" in *Olmstead*. *See generally id.*

33. 277 U.S. 438.

34. *Id.* at 463–66 ("We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.").

agents tapped the phone lines of certain individuals suspected of being involved in the unlawful importation, possession, and sale of liquor.[35] The Court noted that the suspects' telephone wires were tapped without trespassing on any property owned by them, and the information was gathered for many months.[36] The Court reasoned that the "well-known historical purpose of the Fourth Amendment" is to prevent the government from "search[ing] a man's house, his person, his papers, and his effects, and to prevent their seizure against his will."[37] However, the Court found the wiretapping did not constitute an unreasonable search under the Fourth Amendment because there was no physical trespass.[38]

The Court in *Olmstead* failed to recognize the parallels between papers sent in the mail and electric signals sent along a wire. While the Court recognized the technological advancement of telephones as compared to communication through written letters, it was unwilling to extend Fourth Amendment protection to this new technology because the Fourth Amendment was thought to be limited only to searches and seizures of *tangible* property.[39] Following this logic, the Court ruled that there was no search or seizure in listening to the telephone calls because the evidence was collected by the agents using only their auditory perception.[40] Further, the Court reasoned that there was neither an "entry of houses or offices of the defendants" nor a "seizure" of any property.[41]

While the majority did not wish to recognize the technological advancement, Justice Louis D. Brandeis understood that there could be instances in the future where technological advancements trigger Fourth Amendment protection and maintained that Fourth Amendment protections should have been, and would eventually need to be, extended further than the literal text of the Amendment.[42]

3. Post-*Olmstead* Privacy Law

The *Olmstead* decision provided the standard for many years with regard to technology and electronic surveillance. While the Court hesitated to extend

35. *Id.* at 455–57.
36. *Id.* at 457.
37. *Id.* at 463.
38. *Id.* at 463–64.
39. *Id.* at 464.
40. *Id.*
41. *Id.*
42. *Id.* at 474 (Brandeis, J., dissenting) ("The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.").

Fourth Amendment rights to intangible invasions,[43] it drew a bright-line for physical searches.[44] Any physical invasion of the structure of the home "by even a fraction of an inch" was deemed to be a violation of a person's rights.[45] For example, in *Goldman v. United States*,[46] a microphone placed on a wall to eavesdrop on an adjoining room was not considered a search because no physical intrusion of a protected space occurred.[47] However, under the holding in *Silverman v. United States*, a "spike mike"[48] that barely pierced the adjoining wall to capture the same conversation was considered a search.[49] The *Silverman* Court criticized *Olmstead*'s reasoning as being overly limiting while ignoring technological developments that would soon be capable of invading privacy without physically trespassing into constitutionally protected spaces.[50]

In response to the *Olmstead* opinion, Congress passed § 605 of the Federal Communications Act of 1934[51] to regulate wiretapping.[52] However, this law was "grossly ineffective" and was far less protective than the Fourth Amendment.[53] The twentieth century, therefore, saw increased wiretapping

43. *E.g.*, Hoffa v. United States, 385 U.S. 293, 302 (1966) (holding statements made to undercover cops do not violate the Fourth Amendment because "[t]he petitioner . . . was not relying on the security of the hotel room; he was relying upon his misplaced confidence that [the undercover cop] would not reveal his wrongdoing."); Silverman v. United States, 365 U.S. 505, 511–12 (1961) (holding the use of a "spike mike" to monitor conversations occurring among individuals with in a home unconstitutional); Goldman v. United States, 316 U.S. 129, 134–36 (1942) (holding evidence collected by using a detectaphone against an office wall was admissible and did not violate the Fourth Amendment because there was no reasonable assumption that conversations would be confined within the walls of an office), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

44. *See Silverman*, 365 U.S. at 512.

45. *Id.*

46. 316 U.S. at 129.

47. *Id.* at 134–36.

48. *Silverman*, 365 U.S. at 506–07 ("[The spike mike] was a microphone with a spike about a foot long attached to, it together with an amplifier, a power pack, and earphones. The officers inserted the spike under a baseboard in a second-floor room of the vacant house and into a crevice extending several inches into the party wall, until the spike hit something solid 'that acted as a very good sounding board.' The record clearly indicates that the spike made contact with a heating duct serving the house occupied by the petitioners thus converting their entire heating system into a conductor of sound.").

49. *Id.* at 511–12.

50. *Id.* at 511 ("In these circumstances we need not pause to consider whether or not there was a technical trespass under the local property law relating to party walls. Inherent Fourth Amendment rights are not inevitably measurable in terms of ancient niceties of tort or real property law.").

51. Federal Communications Commission Act, Pub. L. 73-416, 48 Stat 1064 (codified as amended at 47 U.S.C. § 605 (2018)).

52. Solove, *supra* note 1, at 1086.

53. *Id.*

and electronic surveillance, as there was not adequate control and oversight when it came to the intersection of surveillance and privacy rights.[54]

This era of virtually unrestricted surveillance was upended by *Katz v. United States*,[55] wherein the Court overturned *Olmstead* and held that a warrant is necessary to wiretap telephone calls made in public telephone booths.[56] In *Katz*, the defendant was in a public telephone booth but did not intend for his conversation to be exposed to the public; therefore, the Court held that he had a reasonable expectation of privacy in the telephone booth.[57] The Court wrote, "[T]he Fourth Amendment protects people, not places."[58] Therefore, "[w]hat a person knowingly exposes to the public, even [if made] in his own home or office," does not receive Fourth Amendment protection.[59] However, the Court continued, "[W]hat he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[60] The Court, after considering the state of technology in 1967, no longer required a physical invasion to constitute a search.[61] Additionally, *Katz* established that searches could occur outside of the home and that a *physical* trespass was no longer necessary to find a Fourth Amendment violation.[62] However, *Katz*'s holding was limited to the content of telephone conversations.[63]

The majority in *Katz* failed to provide a clear test for deciding future Fourth Amendment cases involving technology, however, Justice John Marshall Harlan II's concurrence proposed a framework for future Fourth Amendment violations.[64] This framework consisted of two requirements: "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.'"[65] It took many years for Justice Harlan's framework to gain popularity, but it is now the predominant test that courts utilize when assessing

54. *See id.*
55. Katz v. United States, 389 U.S. 347 (1967).
56. *See id.* at 358–59.
57. *Id.*
58. *Id.* at 351.
59. *Id.*
60. *Id.*
61. *Id.* at 353.
62. *Id.* at 352–53.
63. *Id.*
64. *Id.* at 361 (Harlan, J., concurring).
65. *Id.*

Fourth Amendment issues.[66] The majority's decision established the reasonable expectation of privacy test.[67] "By overruling *Olmstead*, [the Court] . . . established the notion that Fourth Amendment analysis must be sensitive to both the potential for increasing intrusiveness into conventional activities and the evolving landscape of social interchange."[68]

B. The Evolution of the Third-Party Doctrine

The third-party doctrine weakens Fourth Amendment protections when a person voluntarily shares information with a third party, such as the sharing of deposit or withdrawal information with a bank or the sharing of dialed telephone numbers with a phone company.[69] Once the information is shared, the third party is not expected to keep the information secret.[70] Therefore, a person assumes the risk of private information being shared as soon as he or she shares that information with the third party.

Smart home devices, such as home assistants, operate by storing users' data at third-party locations. As technology continues to advance, the third-party doctrine becomes increasingly important for courts to consider when determining how to best protect the privacy of citizens.

---

66. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 33 (2001) ("[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."); California v. Greenwood, 486 U.S. 35, 39 (1988) ("The warrantless search and seizure of the garbage bags left at the curb outside the Greenwood house would violate the Fourth Amendment only if respondents manifested a subjective expectation of privacy in their garbage that society accepts as objectively reasonable."); Smith v. Maryland, 442 U.S. 735, 740 (1979) ("Consistently with *Katz,* this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848, *as recognized in In re* Certified Question of Law, 858 F.3d 591 (Foreign Int. Surv. Ct. Rev. 2016).

67. *Katz*, 389 U.S. at 359.

68. Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 629 (2011).

69. *See* Jennifer Lynch, *Symposium: Will the Fourth Amendment Protect 21st-Century Data? The Court Confronts the Third-Party Doctrine*, SCOTUSBLOG (Aug. 2, 2017), http://www.scotusblog.com/2017/08/symposium-will-fourth-amendment-protect-21st-century-data-court-confronts-third-party-doctrine/.

70. *Id.*

1. Early Third-Party Doctrine Cases

The third-party doctrine is best understood by looking at three major cases: *Couch v. United States*,[71] *United States v. Miller*,[72] and *Smith v. Maryland*.[73]

In *Couch v. United States*, the Court held there was no expectation of privacy in business records turned over to an accountant because a majority of the information was required to be disclosed in an income tax return.[74] Here, an accountant surrendered business and tax information to the Internal Revenue Service ("IRS") that he had received for purposes of filing income tax returns for a taxpayer.[75] Focusing on the content of the information, the Court held that the information handed over to the IRS by the accountant was nothing more than what would be reported for income tax return purposes; thus, there was no Fourth Amendment violation of privacy in the information.[76]

Three years later, in *United States v. Miller*,[77] the Court held there was no reasonable expectation of privacy in an individual's bank records (financial statements, deposit slips, etc.), which contained only information "voluntarily conveyed" to the bank and exposed to its employees in the ordinary course of business.[78] Again, the Court focused on the content of the information and reached the same result as it did in *Couch* because it found the defendant had *no expectation of privacy concerning the information*.[79] The Court stated, "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[80] Therefore, because the bank records were voluntarily conveyed in the ordinary course of business and there was no expectation of privacy, no Fourth Amendment protection applied, and no warrant was required.[81]

---

71. 409 U.S. 322, 335 (1973).

72. United States v. Miller, 425 U.S. 435, 442–44 (1976), *superseded by statute*, Right to Financial Privacy Act of 1978, Pub. L. No. 95–630, 92 Stat 3641 (codified as amended at 12 U.S.C. ch. 35), *as recognized in* Chao v. Cmty. Tr. Co., 474 F.3d 75, 83 (3d Cir. 2007).

73. Smith v. Maryland, 442 U.S. 735, 743–44 (1979), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848, *as recognized in In re* Certified Question of Law, 858 F.3d 591 (Foreign Int. Surv. Ct. Rev. 2016).

74. 409 U.S. at 335.

75. *Id.* at 323–24.

76. *Id.* at 335.

77. 425 U.S. 435.

78. *Id.* at 442.

79. *See id.* at 442–43.

80. *Id.* at 443.

81. *Id.* at 444–45.

Another three years passed before *Smith v. Maryland* was decided.[82] There, the Court held that telephone subscribers did not have a legitimate expectation of privacy in the phone numbers they dialed because users must disclose those numbers to the telephone company in order to complete their call.[83] The Court adopted the two-part analysis proposed by Justice Harlan's concurring opinion in *Katz*, which considered (1) whether an individual has an actual expectation of privacy that he seeks to preserve and (2) whether society recognizes that expectation of privacy as reasonable and justifiable under the circumstances.[84]

As to the first question, the petitioner in *Smith* argued he had an expectation of privacy not because of his conduct but because his telephone use occurred in his home.[85] However, the Court articulated that the location of the call was "immaterial" to Fourth Amendment analysis.[86] The Court reasoned that while petitioner may have intended to keep the contents of his conversation private, his conduct could not preserve the privacy of the number he dialed because the telephone company received the number from users in the same way, regardless of location.[87]

Addressing the second question, the Court pointed out that subscribers must understand that phone companies keep permanent records of the phone numbers dialed for legitimate business purposes, such as billing, and that those numbers appear on the monthly phone bill.[88] Because subscribers were aware that the telephone company was recording the numbers, the Court found the user voluntarily conveyed this information by using the phone.[89] The Court noted that it "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[90] Therefore, because there was no expectation of privacy where the information was voluntarily turned over to a third party, there was no Fourth Amendment protection, and no warrant was required.[91]

Couch, *Miller*, and *Smith* establish two distinct propositions regarding the third-party doctrine.[92] First, voluntarily sharing information with a third party eliminates one's expectation of privacy.[93] It follows that once there is no ex-

82. 442 U.S. 735 (1979).
83. *Id.* at 742.
84. *Id.* at 740 (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).
85. *Id.* at 743.
86. *Id.*
87. *Id.*
88. *Id.* at 742.
89. *Id.* at 743–44.
90. *Id.*
91. *Id.* at 745–46.
92. Strandburg, *supra* note 68, at 638.
93. *Id.*

pectation of privacy, a third party can disclose the information to the government without a warrant.[94] Second, all information stored by a third party is subject to the government's will, even if the third party does not want to turn the information over and even if the information is stored temporarily on third-party servers.[95] This information includes "all transaction data, cell phone location data, social network information, text messages, and data stored in the cloud."[96]

2. Modernization of the Third-Party Doctrine

As technology advanced from landline telephones to cell phones and computers, the third-party doctrine became an increasingly important aspect of technology users' privacy. However, the United States Supreme Court has not accepted technological advancements as willingly as the general public has.

a. Lack of Clarity: *City of Ontario v. Quon*

The Court was hesitant to clarify the concept of privacy expectations in communications made on electronic devices owned by a government employer in *City of Ontario v. Quon*.[97] Here, the question was whether a police officer's personal text messages sent on his government-owned cell phone were protected by the Fourth Amendment from a search by his government employer.[98] The Court ultimately held that the search was reasonable.[99] The Court was concerned about what "emerging technology['s]" role would be in society.[100]

The *Quon* Court looked to the *Katz* Court for guidance. The *Katz* Court relied on "its own knowledge and experience" when deciding a reasonable expectation of privacy in a phone booth existed.[101] However, at the time *Quon* was decided, the Court did not feel it had the necessary knowledge to "elaborate[e] too fully on the Fourth Amendment['s] implications of emerging technology."[102] The Court also noted that the "[r]apid changes in the dynamics of communication and information transmission" caused similar rapid changes "in what society accepts as proper behavior."[103] This holding obscured privacy expectations of electronic communications and what is considered reasonable.

---

94. *Id.*
95. *Id.*
96. *Id.* at 638–39.
97. *See* 560 U.S. 746, 759 (2010).
98. *See id.* at 754; Brief of Respondents at 12, City of Ontario v. Quon, 560 U.S. 746 (2010) (No. 08-1332), 2010 WL 989696, at *12.
99. *Quon*, 560 U.S. at 765.
100. *Id.* at 759.
101. *Id.*
102. *Id.*
103. *Id.*

The Court avoided the issues of whether the officer had a reasonable expectation of privacy in the messages by instead focusing on the impact of office policies concerning the use of his government-provided pager.[104]

b. Steps in the Right Direction: *United States v. Warshak*

In the wake of *Quon*, courts were uncertain as to how the privacy of electronic communications should be handled. Some courts took a narrower interpretation of the third-party doctrine and held there was no expectation of privacy in non-content information, which is information – such as a telephone number or an email address – that is not part of the substance of the communication.[105] However, in *United States v. Warshak*,[106] the U.S. Court of Appeals for the Sixth Circuit took a different approach and held that the government's warrantless search of a small business owner's emails violated the Fourth Amendment because "a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, [an email provider]."[107] Applying the Justice Harlan's two-part analysis in *Katz*, which was adopted in *Smith*, the court reasoned that Warshak had an expectation that his emails would be subject to privacy because the emails encompassed his "entire business and personal life."[108] The court took into account the sensitive nature of the content in the emails and thought it was "highly unlikely that Warshak expected [the emails] to be made public."[109] Therefore, the court found "Warshak had a subjective expectation of privacy in the content[] of [the] emails."[110]

In analyzing the second question, the court discussed the "prominent role" email has taken in modern communication.[111] The court recognized that people use email to "instantaneously" send "sensitive and intimate information,"

104. *See id.* at 760–61.

105. *See, e.g.*, Rehberg v. Paulk, 611 F.3d 828, 842–47 (11th Cir. 2010) (discussing privacy expectations in e-mail and summarizing case law finding no expectation of privacy in non-content information); United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (holding that an individual does not have a protectable expectation of privacy in electronic subscriber information); United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (explaining that there is no Fourth Amendment privacy protection in subscriber information sent to Yahoo!); United States v. Forrester, 512 F.3d 500, 509–10 (9th Cir. 2008) (finding, by analogy to *Smith*'s treatment of telephone numbers, no protectable privacy interest in non-content information and declining, on qualified immunity grounds, to decide whether e-mail content receives Fourth Amendment protection).

106. 631 F.3d 266 (6th Cir. 2010).

107. *Id.* at 288.

108. *Id.* at 284.

109. *Id.*

110. *Id.*

111. *Id.*

document online purchases, and discuss confidential business plans.[112] The court reasoned that if an email address was compromised, one would have access to "an account of its owner's life."[113] Two important principles can be extracted from the court's decision: (1) when information is passed through a communications network, it is necessary to make a Fourth Amendment consideration of whether a person's right to privacy is being violated and (2) it is important to interpret the Fourth Amendment in light of evolving technological progress, otherwise "its guarantees will wither and perish."[114]

The court made two comparisons to justify its reasoning. First, letters in the mail receive Fourth Amendment protection because a government agent cannot read a letter without a warrant.[115] Additionally, letters are handled by a third-party intermediary, the United States Post Office, and still, an officer cannot access a letter in the custody of the Post Office without a warrant.[116] Second, phone calls are handled by a third-party intermediary, the phone company, and yet, these communications cannot be intercepted by a government agent without a warrant.[117] Therefore, the court reasoned that, due to the similarities between email and traditional forms of communication, such as letters and telephone calls, "it would defy common sense to afford emails lesser Fourth Amendment protection."[118] Thus, government agents cannot compel a third party to turn over contents of an email without a warrant.[119]

The Sixth Circuit differentiated its opinion from the United States Supreme Court's opinion in *Miller* by noting *Miller* involved simple business records, whereas there were confidential personal communications at issue in *Warshak*.[120] Additionally, in *Warshak* the information was not viewed "in the ordinary course of business" but rather the third party was an "intermediary . . . [and] not the intended recipient."[121] The Court in *Warshak* understood how society treated technology and applied Justice Harlan's two-step analysis from

112. *Id.*

113. *Id.*

114. *Id.* at 285; *see also* Kyllo v. United States, 533 U.S. 27, 34 (2001) (reasoning technological progress must not be allowed to "erode the privacy guaranteed by the Fourth Amendment.").

115. United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy . . . .").

116. *Warshak*, 631 F.3d at 285.

117. *See* Katz v. United States, 389 U.S. 347, 359 (1967).

118. *Warshak*, 631 F.3d at 285–86. This same reasoning was used by the Ninth Circuit in *United States v. Forrester*. 512 F.3d 500, 511 (9th Cir. 2008) ("The privacy interests in [mail and email] are identical.").

119. *Warshak*, 631 F.3d at 288.

120. *Id.* at 287–88.

121. *Id.* at 288.

Katz, as adopted in *Smith*, in reaching a result that protected electronic communications.[122] This bold analysis was a sign that the future of the third-party doctrine may be evolving to accept a more technology-friendly standard.

III. RECENT DEVELOPMENTS

In 2012, the United States Supreme Court first indicated that it recognized the need for the third-party doctrine to be reevaluated to better assess privacy rights in relation to new technological advancements. In *United States v. Jones*,[123] the Court held that Global Positioning System ("GPS") monitoring constituted a search because it involved the government's trespass onto private property "for the purpose of obtaining information."[124] While the opinion itself did not implicate the third-party doctrine, five Justices, in concurring opinions, indicated a willingness to rethink parts of the doctrine.[125] Specifically, Justice Sonia M. Sotomayor noted that, given the continuing evolution of technology, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[126] She went on to say the third-party doctrine is

> ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[127]

Additionally, Justice Samuel A. Alito, Jr. articulated that "[n]ew technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."[128]

Following the *Jones* concurrences, "state and federal courts have increasingly rejected the government's attempts to extend *Smith* to new forms of

122. *Id.* at 285.
123. 565 U.S. 400 (2012).
124. *Id.* at 404–05.
125. *See id.* at 417 (Sotomayor, J., concurring); *id.* at 427–28 (Alito, J., concurring).
126. *Id.* at 417 (Sotomayor, J., concurring).
127. *Id.*
128. *Id.* at 427 (Alito, J., concurring).

data."[129] For example, in *United States v. Graham*,[130] the U.S. Court of Appeals for the Fourth Circuit held that a warrantless, extended collection of defendants' cell-site data by the government was an unconstitutional search, but this holding was later reversed en banc.[131] In *United States v. Davis*,[132] the U.S. Court of Appeals for the Eleventh Circuit found a reasonable expectation of privacy in "even one point of cell[-]site location data," but this holding was also reversed en banc.[133] Further, eleven state supreme courts[134] have explicitly rejected the third-party doctrine, and ten[135] others have indicated a possibility of doing so in the future.[136] However, the reversals of *Graham* and *Davis* show that the United States Supreme Court must be the first to update the third-party doctrine before lower courts will be able to do so.

Some thought the Court would update the doctrine with its decision of *Riley v. California*.[137] The Court in *Riley* held that a warrant was required to search a cell phone when the cell phone was seized incident to an arrest.[138] In so holding, the Court declined to extend the traditional Fourth Amendment exception for searches incident to arrest,[139] as established by *United States v. Robinson*.[140] In *Robinson*, the Court upheld the search of a cigarette pack recovered incident to an arrest.[141] The question in *Riley* was whether searching

---

129. Hanni Fakhoury, Smith v. Maryland *Turns 35, but Its Health Is Declining*, ELEC. FRONTIER FOUND. (June 24, 2014), https://www.eff.org/deeplinks/2014/06/smith-v-maryland-turns-35-its-healths-declining.

130. 796 F.3d 332 (4th Cir. 2015), *reh'g granted* 824 F.3d 421 (4th Cir. 2016), *abrogated by* Carpenter v. United States, 138 S. Ct. 2206 (2018).

131. *Id.* at 338.

132. 754 F.3d 1205 (11th Cir. 2014), *reheard and vacated by* 785 F.3d 498 (11th Cir. 2015).

133. *Id.* at 1216.

134. The state supreme courts in California, Colorado, Florida, Hawaii, Idaho, Illinois, Montana, New Jersey, Pennsylvania, Utah, and Washington have all rejected the federal third-party doctrine. Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 395 tbl.1 (2006).

135. The state supreme courts in Alaska, Arkansas, Indiana, Massachusetts, Minnesota, New Hampshire, Oregon, South Dakota, Texas, and Vermont have indicated that they might reject the federal third-party doctrine. *Id.* at 395 tbl.2.

136. *Id.* at 376. These numbers are based on Henderson's survey of cases surrounding this topic in each state. *Id.*

137. 134 S. Ct. 2473 (2014).

138. *Id.* at 2495.

139. Clifford S. Fishman, *Searching Cell Phones After Arrest: Exceptions to the Warrant and Probable Cause Requirements*, 65 RUTGERS L. REV. 995, 1002 (2013) ("Police may conduct a search without first obtaining a warrant 'when the exigencies of the situation make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment.'").

140. 414 U.S. 218 (1973).

141. *Riley*, 134 S. Ct. at 2484 (citing *Robinson*, 414 U.S. at 236).

a smart phone could be considered an invasion of privacy equivalent to the search of a cigarette pack and whether the amount of personal data stored on the smart phone changed the analysis.[142] In making its decision, the Court assessed, on the one hand, "the degree to which [the search] intrudes upon an individual's privacy and, on the other, the degree to which [the search] is needed for the promotion of legitimate governmental interests."[143]

The Court noted that law enforcement officials are permitted "to examine the physical aspects of a phone to ensure that it will not be used as a weapon"[144] but cannot examine its contents.[145] The Court reasoned that data on cell phones differs in both a "quantitative and a qualitative sense" from other objects that an arrestee may carry.[146] The Court deemed this an important issue because "many of the more than [ninety percent] of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives."[147] The Court noted that privacy interests were further complicated because data that appears to be stored on cell phones may actually be stored on a remote server that is maintained and operated by a third party.[148]

The government, relying on *Smith*, presented the argument that police should at least be able to look at the cell phone's call log.[149] However, the Court rejected this argument and distinguished cell phone call logs from the call logs discussed in *Smith* because cell phone "call logs typically contain more than just [a] phone number[]."[150] This reasoning implies that the more informative the information is, the more it should be entitled to Fourth Amendment protection. The Court reasoned that "[t]he 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."[151] Recognizing the need for police to search cell phones in appropriate instances, the Court held that police officers must first get a warrant before searching a cell phone seized incident to an arrest.[152]

While *Riley* represented a step in the right direction with regard to how technology is treated under the Fourth Amendment, its holding is relatively

142. *Id.*

143. *Id.* (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

144. *Id.* at 2485.

145. *Id.*

146. *Id.* at 2489 ("One of the most notable distinguishing features of modern cell phones is their immense storage capacity.").

147. *Id.* at 2490 (alteration in original) ("Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: 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 – unless the phone is.").

148. *Id.* at 2491.

149. *Id.* at 2492.

150. *Id.* at 2492–93.

151. *Id.* at 2495.

152. *Id.*

narrow because it is limited to searches incident to arrest.[153] Even so, the Court's dicta was monumental regarding the modernization of the third-party doctrine.

In *Carpenter v. United States*,[154] the Court held that, in narrow circumstances,[155] information held by third parties may still be subject to Fourth Amendment protection.[156] Here, four men were arrested in connection with a string of armed robberies.[157] One of the men confessed and gave police his personal cell phone number and the cell phone numbers of the others allegedly involved.[158] The prosecutors used this information to apply for court orders – not warrants – under the Stored Communications Act[159] to obtain records for Carpenter and the other suspects from each of their respective cell phone carriers.[160] The orders were granted for Carpenter's carriers to disclose cell-site sector information at "call origination and at call termination for incoming and outgoing calls" during the designated time period.[161] Based on the recovered information, Carpenter was charged and convicted.[162] When Carpenter challenged the government's use of the cell-site information without a warrant, the

153. *Id.* at 2489 n.1 (alteration in original) ("[T]hese 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.").

154. 138 S. Ct. 2206 (2018).

155. *Id.* at 2220 ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time [cell-site location information] or 'tower dumps' (a download of information on all the devices that connected to a particular cell-site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.").

156. *Id.* at 2222.

157. *Id.* at 2212.

158. *Id.*

159. Stored Communications Act, Pub. L. No. 99–508, 100 Stat 1848 (1986) (codified as amended at 18 U.S.C. §§2701–2712 (2018)); *see also* HANNAH BLOCH-WEHBA & JENNIFER R. HENRICHSEN, ELECTRONIC COMMUNICATIONS SURVEILLANCE: WHAT JOURNALISTS AND MEDIA ORGANIZATIONS NEED TO KNOW 10 (2017), https://www.rcfp.org/wp-content/uploads/imported/SURVEILLANCE.pdf ("The Stored Communications Act authorizes the government to require providers of electronic communications services to disclose both the substantive contents of stored communications as well as the metadata records associated with those communications (e.g., email dates, times, and header information, including 'to' and 'from' addresses).").

160. *Carpenter*, 138 S. Ct. at 2212.

161. *Id.*

162. *Id.* at 2212–13.

Sixth Circuit held that he had no expectation of privacy in the information because this information was shared with a third party: his wireless carriers.[163]

On appeal to the United States Supreme Court, the Court compared the cell-site data to that of GPS monitoring, which resulted in "detailed, encyclopedic, and effortlessly compiled" information.[164] The Court acknowledged the third-party doctrine and further acknowledged that Carpenter continuously revealed his location to his carrier.[165] However, the Court declined to extend *Smith* and *Miller* because it determined that detailed information, such as the cell-site data, belonged in a "qualitatively different category" than telephone numbers or bank records.[166] Unlike GPS monitoring, a cell phone is "almost a feature of human anatomy . . . [which] tracks nearly exactly the movements of its owner."[167] No matter who the suspect may be, it is as if "he has effectively been tailed every moment of every day for five years," and "[o]nly the few [people] without cell phones could [avoid] this tireless and absolute surveillance."[168]

The fact that the cell-site information was held by a third party did not eliminate Carpenter's claim to Fourth Amendment protection, even though the records were business records created and maintained by the wireless carriers.[169] The location data was not truly voluntarily shared, as cell phones continuously log cell-site data with "no affirmative act on the part of the user beyond powering up."[170] The Court reasoned that the key consideration was the "deeply revealing nature" of the information as well as its "depth, breadth, . . . comprehensive reach, and the inescapable and automatic nature of its collection."[171] Therefore, the cell-site data that prosecutors had obtained without a warrant was classified as a search subject to Fourth Amendment protection.[172]

However, the Court was careful to note that its narrow decision did not disturb the application of *Smith* and *Miller* or "call into question conventional surveillance techniques and tools, such as security cameras" or "business records that might incidentally reveal location information."[173]

IV. DISCUSSION

Under the current framework, smart home device data lacks Fourth Amendment protection. However, recent cases show that the United States

163. *Id.* at 2213.
164. *Id.* at 2216.
165. *Id.* at 2216–17.
166. *Id.*
167. *Id.* at 2218 (citation omitted).
168. *Id.*
169. *Id.* at 2216–17.
170. *Id.* at 2220.
171. *Id.* at 2223.
172. *Id.*
173. *Id.* at 2221.

Supreme Court may be willing to take another look at the third-party doctrine in order to uphold Fourth Amendment protections in light of these technological advancements.

A. Smart Home Devices Under the Current Third-Party Doctrine and Privacy Law

People in the Information Age have the ability "to communicate, transfer and share information[, and] access data" from anywhere.[174] Smart home devices are in their early stages but can already control lights, televisions, thermostats, and monitor a home to ensure it is maintained in an efficient and safe manner. These devices provide several benefits, such as offering a higher standard of living for relatively low costs, assisting the elderly or disabled, and providing a sense of security. The merchants who produce these devices store user data with the intention of using the data to access devices remotely, develop their products, and turn a profit by selling the data to advertisers. These devices can make day-to-day lives easier for all who choose to use them. But many consumers do not realize the consequences that stem from allowing such data collection in their homes.[175] Three main consequences are "(1) the effect on individual behavior and well-being, (2) the effect on corporations and their ability to do business in new and unusual ways, and (3) the effect on government action."[176]

The third-party doctrine, as it currently stands, implies that a majority of information provided by a user to a third party loses Fourth Amendment protection under the reasonable expectation of privacy theory.[177] This doctrine's rationale is that by giving the information to a third party, the giver loses the right to privacy in that information. "[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[178] Thus, by using smart home devices, a user voluntarily turns over personal data to third parties.

For example, consider a voice assistant device, such as the Amazon Echo or Google Home. These devices control music and lighting, order products,

174. Solove, *supra* note 1, at 1088.

175. *See* Jillisa Bronfman, *Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population*, 14 DUKE L. & TECH. REV., 192, 192–93 (2016).

176. *Id.* at 193–94.

177. Ferguson, *supra* note 20, at 575.

178. Smith v. Maryland, 442 U.S. 735, 743–44 (1979), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848, *as recognized in In re* Certified Question of Law, 858 F.3d 591 (Foreign Int. Surv. Ct. Rev. 2016); *see also* United States v. Miller, 425 U.S. 435, 442–44 (1976), *superseded by statute*, Right to Financial Privacy Act of 1978, Pub. L. No. 95–630, 92 Stat 3641 (codified as amended at 12 U.S.C. ch. 35), *as recognized in* Chao v. Cmty. Tr. Co., 474 F.3d 75, 83 (3d Cir. 2007).

and even answer questions merely by using a "wake word"[179] followed by the desired command.[180] When a user makes a request, the voice assistant records the user's speech, transmits the recording to its home server to correctly process the request, and stores the recording on the company's servers.[181] For the device to recognize a "wake word" when used, the device must always be listening.[182] Some brands of devices overwrite background chatter data that is not associated with a request, while others store all the data.[183] Surveillance systems operate similarly. For example, the "Nest Cam" records and transmits data continuously until it is manually turned off.[184] Under the current third-party doctrine, these devices essentially eliminate Fourth Amendment protections associated with the home by voluntarily conveying data to a third party. Therefore, police could gain access to the data without a warrant because gaining access would likely not constitute a search under the current third-party doctrine.[185]

These devices seem somewhat similar to the cell-site data discussed in *Carpenter*. The most important similarity is that users have little to no control over data being shared to the third party. Data automatically transmits by merely turning on many of these devices. Smart water meters, smart watches, some brands of home assistants, and home video security systems are always listening and/or recording.[186] Some of this data is also "deeply revealing in

179. A wake word is a word that tells the smart home device the user is specifically talking to the device. This word puts the smart home device on notice that the user is about to give a command.

180. Rich Jaroslovsky, *Google Home vs. Amazon Echo Is a Battle of Smarts and Skills*, OBSERVER (Jan. 17, 2017, 7:00 AM), https://observer.com/2017/01/google-home-versus-amazon-echo-review/.

181. Christopher Mele, *Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concerns*, N.Y. TIMES (Dec. 28, 2016), https://www.nytimes.com/2016/12/28/business/amazon-echo-murder-case-arkansas.html.

182. *Id.*

183. *See, e.g.*, Mele, *supra* note 181; Michael Justin Allen Sexton, *Cortana Is Listening*, TOM'S HARDWARE (Aug. 10, 2015, 2:00 PM), http://www.tomshardware.com/news/cortana-is-watching,29791.html.

184. STACEY GRAY, FUTURE OF PRIVACY FORUM, ALWAYS ON: PRIVACY IMPLICATIONS OF MICROPHONE-ENABLED DEVICES 6 (2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf.

185. *See generally* Couch v. United States, 409 U.S. 322 (1973); Smith v. Maryland, 442 U.S. 735, 743–44 (1979), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848, *as recognized in In re* Certified Question of Law, 858 F.3d 591 (Foreign Int. Surv. Ct. Rev. 2016); United States v. Miller, 425 U.S. 435, 442–44 (1976), *superseded by statute*, Right to Financial Privacy Act of 1978, Pub. L. No. 95–630, 92 Stat 3641 (codified as amended at 12 U.S.C. ch. 35), *as recognized in* Chao v. Cmty. Tr. Co., 474 F.3d 75, 83 (3d Cir. 2007).

186. *See* Larry Greenemeier, *Alexa, What Are You Doing with My Family's Personal Info?*, SCI. AM. (Jan. 15, 2018), https://www.scientificamerican.com/article/alexa-what-are-you-doing-with-my-familys-personal-info/.

nature," as in *Carpenter*.[187] Home assistants record all conversations occurring in a home, when users are home, users' likes and dislikes, and users' personal preferences.[188]

However, these devices likely do not fall under the narrow holding of *Carpenter* because there are key differences between smart home devices and cell-site date. The most important difference is that, unlike cell phones, these devices do not follow an individual's every movement. Devices such as home assistants can only pick up on what can be heard in a certain location of a home. Another key difference is that, unlike cell phones, smart home devices are not nearly as common. The United States has a population of 326 million people and *396 million* cell phone service accounts,[189] with ninety-five percent of Americans owning a cell phone.[190] The Court understands that cell phones are a way of life and that it is difficult to function in our society without a cell phone. In contrast, estimates suggest there are a total of 40.3 million smart homes in the United States.[191] This estimate includes devices that assist with home entertainment, control and connectivity, energy management, comfort and lighting, smart appliances, and security.[192] Even with all of these categories combined, smart devices are vastly less popular in 2018 than cell phones.[193] However, every year the number of smart homes continues to increase.[194] Sixty-nine million homes are predicted to be smart homes by 2022.[195]

Cell phones were once the new, up-and-coming technology. However, it is only after ninety-five percent of Americans were recognized as using cell phones that courts started to interpret the Fourth Amendment to catch up with the privacy issues surrounding these devices. Smart home devices are on a fast-upward trend and will likely soon be just as common as cell phones are today. For this reason, it is important to prepare for the reality of the future. Smart home device data is very valuable, as it can give insights into who a person is, how a person behaves, what tastes a person has, and what a person's intentions are. When this data is in the hands of companies interested in selling products, this exchange of information may not seem concerning; however, when this data is in the hands of government and law enforcement officials, there may be significant concerns.

---

187. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

188. GRAY, *supra* note 184, at 6, 10.

189. *Id.* at 2223.

190. *Mobile Fact Sheet*, PEW RES. CTR. (Feb. 2, 2018), http://www.pewinternet.org/fact-sheet/mobile/.

191. *Smart Home*, STATISTA, https://www.statista.com/outlook/279/109/smart-home/united-states (last visited Oct.16, 2018).

192. *See id.*

193. *Compare Mobile Fact Sheet, supra* note 190 (stating that ninety-five percent of Americans own smart phones as of 2018), *with Smart Home, supra* note 191 (stating that current smart home penetration is thirty-two percent).

194. *Smart Home*, *supra* note 191.

195. *Id.*

Police have used data from Fitbits,[196] home video surveillance,[197] smart water meters, cell phones, and much more to gather evidence for cases.[198] The data on many smart home devices is only as protected as the third party holding the information desires. For example, in the murder investigation discussed *supra*, if Amazon's policies had been different, there would have been nothing stopping it from handing over the data to police – with or without a warrant.[199] Once the information is out, a user no longer has the power to control who can see or use the information. Users are left depending on the third parties collecting this information to have policies in place that protect their private information. This is worrisome, as smart home devices become more common in daily lives and many users are uninformed as to the possible ramifications of using these devices.

B. Updating the Third-Party Doctrine to Reflect Fourth Amendment Protections

When it comes to smart home devices, there are two main privacy rights at issue: (1) the right to exercise control over a user's personal information and (2) the right to notice and consent for the distribution of such personal information – i.e., the right to be free from abuse of private data. To protect these important rights, the third-party doctrine should provide a framework that reflects the technologies available – technologies that allow third parties access to a person's home and to his or her most private information in ways that could not have been fathomed at the time the Fourth Amendment was written.[200] Over the years, the United States Supreme Court has interpreted the Fourth Amendment to protect a person's right to privacy beyond the pre-technological world that existed at the time the Constitution was ratified.[201] This included

196. Amanda Watts, *Cops Use Murdered Woman's Fitbit to Charge Her Husband*, CNN, https://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html (last updated Apr. 26, 2017, 2:58 PM).

197. Trevor Timm, *The Government Just Admitted It Will Use Smart Home Devices for Spying*, GUARDIAN (Feb. 9, 2016, 3:29 PM), https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government.

198. *See, e.g.*, Watts, *supra* note 196; Kathryn Gilker, *Bentonville Police Use Smart Water Meters as Evidence in Murder Investigation*, 5NEWS (Dec. 28, 2016), https://5newsonline.com/2016/12/28/bentonville-police-use-smart-water-meters-as-evidence-in-murder-investigation/; Timm, *supra* note 197; Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY (Aug. 24, 2015), https://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/.

199. *See supra* text accompanying notes 10–13.

200. *See* Ferguson, *supra* note 20, at 566.

201. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2477 (2014) (smartphones); Kyllo v. United States, 533 U.S. 27, 34–37 (2001) (interior of home from thermal imagers); United States v. Karo, 468 U.S. 705, 716 (1984) (beepers); Katz v. United States, 389 U.S. 347, 351–52 (1967) (telephones).

expanding the Fourth Amendment's protections to cars, telephones, and tracking devices.[202] *Carpenter* represented a step in the right direction; however, as with *Riley*, it has a narrow holding that still leaves many types of private data vulnerable under the current third-party doctrine.

The United States Supreme Court has made the following two principles clear in its jurisprudence. First, the home is a private space where a person has a right to "retreat . . . and there be free from unreasonable governmental intrusion."[203] Second, "[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[204] When read together, these principles support the following conclusion: Even though the data collected by smart home devices is stored by third parties, it is intended to be private and can only be collected from inside the home. Therefore, if a "state's corresponding obligation to respect the home's 'wellbeing, tranquility, and privacy' is an interest 'of the highest order in a free and civilized society,'"[205] then the data collected via smart home devices should receive the same protection as telephone calls.

In *Jones*, Justice Sotomayor and Justice Alito focused on the personal information revealed from the GPS device at issue in their concurrences.[206] There, the procurement of the tracking information was considered a search based solely on the informational exposure that resulted – it was not about the car itself but rather about the information that was conferred based on the car's travels. The majority's discussion in *Riley* and Justice Sotomayor's concurring opinion in *Jones* foreshadow the future of the third-party doctrine and Fourth Amendment protections in the context of technological advancements.

Technology in the twenty-first century goes above and beyond the technology in existence at the time *Smith* was decided. The type of information being conveyed by these devices is vastly more personal and private than the mere dialing of phone numbers. Smart devices can potentially record every conversation in a home and store it for an unlimited amount of time.[207] The companies storing this data can create a profile for users, including:

---

202. *See supra* note 201.

203. Silverman v. United States, 365 U.S. 505, 511 (1961).

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

205. Jordan C. Budd, *A Fourth Amendment for the Poor Alone: Subconstitutional Status and the Myth of the Inviolate Home*, 85 IND. L.J. 355, 401 (2010) (quoting Carey v. Brown, 447 U.S. 455, 471 (1980)).

206. Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239, 1249 (2012) ("The concurrences in *Jones* underscored that in the information age, defendants are less concerned about intrusions upon their real property and more concerned about intrusions upon their information." (italics added)).

207. *See* Rory Carroll, *Goodbye Privacy, Hello 'Alexa': Amazon Echo, the Home Robot Who Hears It All*, GUARDIAN (Nov. 21, 2015), https://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud.

> health profile (health monitoring apps), whereabouts (calendar), activities (to-do lists), political leanings (which news sites [he/she] frequents), and even possibly innermost thoughts (think of the one-off Google or WebMD searches you would prefer not to broadcast).[208]

This is not the content-less type of information discussed in *Smith*. There, the information did not contain content – it merely contained numbers.[209] Therefore, there was no reasonable expectation of privacy, whereas, the data at issue with smart home devices contains a vast amount of personal information, which, under the current framework, cannot be protected by a user.[210]

This data should be protected, and a warrant should be required to access this information because of the amount of sensitive material that these smart home devices transmit. In *Jones*, it was not the car but the information gained from the car that was a problematic invasion of privacy. Here, it is not the home but the information gained from inside the home through technology that poses a grave threat to Fourth Amendment protections of persons across the country. Before modern technology, personal documents and records were stored in the home or at the office – such as financial records, health records, personal letters, photographs, and more. These documents are now stored electronically on a computer and are likely backed up to a "cloud."[211] Twenty-first-century technology expands beyond the walls of the home, and the most intimate details of people's lives are stored in electronic databases that cannot be contained within the physical boundary of the home.

The traditional reasonable expectation of privacy test, which focuses on the physical boundaries of the home and office with exceptions for publicly disclosed information, can be "reconceptualized as only protecting the information secured . . . from others."[212] Under this traditional doctrine, the concept of privacy would be constrained to what is "inside" the device rather than including the device itself. Therefore, individuals could only claim a reasonable

---

208. Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1940 (2017).

209. Smith v. Maryland, 442 U.S. 735, 742 (1979), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848, *as recognized in In re* Certified Question of Law, 858 F.3d 591 (Foreign Int. Surv. Ct. Rev. 2016).

210. *See id.*

211. Int'l Bus. Machs. Corp. v. Visentin, No. 11 CIV. 399(LAP), 2011 WL 672025, at *5 (S.D.N.Y. Feb. 16, 2011), *aff'd*, 437 Fed. App'x 53 (2d Cir. 2011) ("Cloud computing allows businesses and individuals to use the Internet to access software programs, applications, and data from computer data centers managed by providers . . . ."). Essentially a cloud allows a user to store documents, photos, multi-media, and more in one location that can be accessed as long as a user has an internet connection and correct username and password credentials. *What is Cloud Computing?*, IBM, https://www.ibm.com/cloud/learn/what-is-cloud-computing (last visited Oct. 16, 2018). This "cloud" is stored by a third party who provides the service for customers. *Id.*

212. Ferguson, *supra* note 20, at 607.

expectation of privacy by taking steps to protect that information; this is largely because voluntarily disclosing the information means it would no longer fall under the Fourth Amendment's protection.

The groundwork for reconceptualizing the reasonable expectation of privacy test has already been laid, as the third-party doctrine's underlying principle focuses on the *content* of the information shared.[213] For example, in *Smith*, the Court concluded that the phone numbers at issue did not constitute sensitive information and that no Fourth Amendment violation had occurred.[214] In so concluding, the Court differentiated the facts of *Smith* from *Katz*, noting that the content of the phone calls was not recorded.[215] Further, in *Miller*, the financial documents were available to all bank employees in the ordinary course of business, and therefore, the Court held such documents did not contain "sensitive" information. Additionally, in *Carpenter*, the Court focused solely on the type of information at issue and whether a user had a lack of control over the transmission of that information. The holdings of the Court in each of these cases turned on what type of content was being conferred and not what physical boundaries were being implicated.

In the Information Age, it is becoming increasingly difficult to decline turning over personal information because "[w]e must 'plug in' to join in. . . . [W]e must establish relationships with a panoply of companies."[216] So, when hearing cases that involve smart home devices and the third-party doctrine, the Court should apply the reasonable expectation of privacy test and look at the specific type of content in question. Only then should the Court determine whether the type of information at issue holds an expectation of privacy.

V. CONCLUSION

The third-party doctrine has existed for many years. It has survived the ever-evolving changes of technology into the twenty-first century. However, as information-sharing technologies – like smart home devices – become more prevalent, it becomes necessary to update the third-party doctrine to preserve the integrity of the Fourth Amendment right to privacy. Justice Sotomayor stated in her concurring opinion in *Jones* that the third-party doctrine is "ill-suited to the digital age."[217] Further, Justice Alito articulated in his concurring opinion in *Jones*, "[E]ven if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."[218] Justice Alito understood that a person should not be forced to choose between participating in modern life and maintaining one's right to privacy with respect to his or her personal information.

213. *See Smith*, 442 U.S. at 741–42.
214. *Id.*
215. *Id.*
216. Solove, *supra* note 1, at 1089.
217. *Id*. at 417 (Sotomayor, J., concurring).
218. United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring).

When looking back at the cases that developed the third-party doctrine, it is clear that these cases were based on careful inquiries into the *type* of information being conveyed. This reasoning should not be overlooked when considering cases involving future technologies. The United States Supreme Court's time as an idle observer of Fourth Amendment jurisprudence in the Information Age must come to an abrupt end; the time for the Court to once again step into the arena of individual privacy and return the analysis to a context-specific framework that will appropriately account for continually evolving technology is *now*.