Third-Party Doctrine: The Threat of the Digital Age

Amarildo Haxhiu*

Abstract: The evolution of the Third-Party Doctrine, its impact on the Fourth Amendment, and its current iteration in the modern digital age is evaluated through a number of precedent cases. The paper will start with the principal of reasonable expectation of privacy, established in *Katz v. United States*, and carry onward into the foundation of the Third-Party Doctrine in *United States v. Miller* and *Smith v. Maryland*, the Court questioning the viability of the doctrine in *United States v. Jones*, and perhaps shifting its outlook in *Carpenter v. United States*. The paper will analyze the Third-Party Doctrine concerns through the *Carpenter* balancing test and conclude with the possible benefits and detriments in applying such a test.

Keywords: Fourth Amendment; criminal procedure; Third-Party Doctrine; balancing test; Supreme Court.

1. *Introduction*

George Orwell boldly wrote, "[a]lways eyes watching you and the voice enveloping you. Asleep or awake, indoors or out of doors, in the bath or bed – no escape. Nothing was your own except the few cubic centimeters in your skull"[1]. Written more than half a century ago, these words ring potentially true and meaningful today and in different contests, too. Nowadays citizens must face multiple privacy risks, as they seem not totally aware of Government programs regularly recording citizens data while endangering Constitutional freedoms[2]. The Government can access information without a warrant and, considering the abundance of information that is constantly shared through several devices, such as cell phones most people should re-evaluate their attitude towards sharing personal data[3].

Concerns are further intensified when large corporations, such as Google and Amazon, collect massive amounts of customers data in their servers[4]. Cloud computing, of which both companies are promi-

---

* Amarildo Haxhiu is a Juris Doctor student at Western Michigan University Cooley Law School and an intern at the Public Defender Office in Ann Arbor, Michigan. He holds his Bachelor of Arts in Political Sciences and Government from Wayne State University.

1. George Orwell, *1984* (Secker & Warburg 1949).

2. See *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor concurring: "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse").

3. See *id.* at 418 (Sotomayor concurring: "I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year").

4. See *Carpenter v. United States*, 138 S. Ct. 2206, 2262 (2018) (Gorsuch dissenting: "Countless Internet companies maintain records about us and, increasingly, for us.

nent players, users can store documents and access them from multiple devices without the necessity to expand their computer data storage[5]. Such documents might range from an innocuous list of grocery items, to detailed banking records, medical records, to culminate to an individual's private diary[6]. In *Riley*, Chief Justice John G. Roberts Jr. appropriately mentioned that:, "[cellphones] could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or, newspapers"[7]. Our homes have welcomed objects embedded with computing systems connected to the internet that monitor our health, and our safety depends on them[8]. The Government cooperates with private companies to combine data and to build profiles of individuals: their habits, their likes and dislikes, their daily movements and routines, and much more[9].

The Third-Party Doctrine – a legal justification used to obtain such information – states that a person has no reasonable expectation to privacy on information shared voluntarily with others, whether it concerns bank details, colleagues, or even telecommunications providers[10]. Most individuals would claim that they never wished to make such information available to the Government, but the latter would reply that the information is admittedly and voluntarily shared with third parties[11]. This argument is misleading. Individuals could theoretically hide their money under their mattresses or send letters instead of emailing, but such measures would prove excessively burdensome, if not incompatible with today's society. As the modern world progresses, the legal community should look to *Carpenter*. Expanding the *Carpenter* decision to cover the Third-Party Doctrine could be an adequate remedy.

Even our most private documents – those that, in other eras, we would have locked safely in a desk drawer or destroyed – now reside on third party servers").

5. See *id.*
6. See *id.*
7. *Riley v. California*, 573 U.S. 373, 393 (2014).
8. See *id.*
9. See *id.*
10. See *United States v. Miller*, 425 U.S. 435 (1976).
11. See *Carpenter*, 138 S. Ct. 2206, 2220 (2018).

2. *Background*

The evolution of the Third-Party Doctrine, its impact on the Fourth Amendment and its current iteration in the modern digital age will be evaluated through a number of precedents. The following section will examine the principle of reasonable expectation of privacy, established in *Katz v. United States*, and carry on into the foundation of the Third-Party Doctrine in *United States v. Miller* and *Smith v. Maryland*, the Court's questioning of the viability of the doctrine in *United States v. Jones*, and its shifting outlook in *Carpenter v. United States*. The concerns arising from the Third-Party Doctrine will be analyzed through the Carpenter balancing test and, in the final part, the benefits and detriments of such test will be examined.

2.1. *Birth of the Third-Party Doctrine*

2.1.1. *Dawn of a New Age:* Katz v. United States

The current precedent on privacy was established in *Katz v. United States*. The main facts of the case revolved around the Government placing a listening device on a payphone to listen to the defendant's conversation. By doing so, the Government was found in violation of the defendant's Fourth Amendment rights. In what later became the bright-line rule, Justice Harlan wrote that, to have violation of Fourth Amendment rights, there is a requirement "first that a person have exhibited an actual expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as reasonable"[12]. By listening to the conversation without a warrant, the Government had violated the Fourth Amendment Search and Seizure Clause. The Court distanced itself from previous rulings of constitutionally protected areas and solidified the Fourth Amendment as guardian of people, rather than places[13]. Nevertheless, the Court clarified that whatever the individual shares publicly is not protected by the Fourth Amendment[14]. The era of the Third-Party Doctrine started.

12. *Katz v. United States*, 389 U.S. 347, 360 (1967).
13. See *id*. at 351 (declining to adopt government's suggested standard).
14. See *id*.

2.1.2. *Third-Party Doctrine Takes Shape:* United States v. Miller *and* Smith v. Maryland

Following *Katz*, in *United States v. Miller*, Mitch Miller was convicted of running an unregistered distillery and failing to pay taxes. The Government had obtained bank records and checks with an allegedly defective *subpoena*[15]. Miller moved to suppress the evidence as a violation of his Fourth Amendment right against "unreasonable searches and seizures"[16]. Relying on *Katz*, the Court held that Miller had no expectation of privacy[17]. They reasoned that, since Miller had given the information to the bank –a third party–voluntarily, the documents no longer belonged to him and were now property of the bank. The Court established a concrete rule concerning expectation of privacy on documents voluntarily surrendered to third parties: individuals have no legitimate expectation of privacy, and there is no violation of Fourth Amendment unreasonable searches and seizures when the individual voluntarily surrenders information to third parties.

In *Smith v. Maryland*, the Court affirmed the rule established in *Miller*. In *Smith*, after a robbery, the victim was continually receiving threatening phone calls from the defendant who identified himself as the robber. On one particular occasion, the defendant asked the victim to step outside, and slowly drove past her home. The victim described the defendant and the car to the police, who later identified him by tracing the license plate number. The Government, without a warrant, requested the telephone company to install a pen register on the victim's telephone. The pen register identified that the calls originated from the defendant's home. Based on the calls, and additional evidence, police obtained a search warrant. The search revealed a phone book, which indicated the victim's name and phone number[18]. The defendant was arrested on the basis of such evidence[19]. Defendant sought to suppress the evidence based on a "legitimate expectation of

15. See *United States v. Miller*, 425 U.S. 435 (1976).
16. *Id.* at 439.
17. See *id.* at 442.
18. See *Smith v. Maryland*, 442 U.S. 735 (1979).
19. See *id.*

privacy"[20], arguing that the installation of the pen register and the identification of dialed numbers constituted a violation of one's legitimate expectation of privacy[21].

Using the rule established in *Katz*, the Court held that the defendant, under the Third-Party Doctrine, had no legitimate expectation of privacy[22] in the numbers that he dialed, since all users must display such numbers to the telephone company, and the subjective expectation that these would remain private was not something society would be prepared to recognize as reasonable[23]. Based on *Miller*, the Court concluded that the defendant assumed a risk by voluntarily conveying information to the third party[24].

In a separate opinion, and what can only be called an ominous allusion to future intrusions by the Government through the tools of third parties, Justice Brennan stated:

> The numbers dialed from a private telephone – although certainly more prosaic than the conversation itself – are not without "content". Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long-distance numbers they have called. This is not because such a list might in some sense be incriminating, but 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[25].

Similarly, Justice Marshall addressed the argument of assumption of risks. He stated, "unless a person is prepared to forgo use of what for

---

20. *Id.* at 741 ("Petitioner's claim, rather, is that, notwithstanding the absence of a trespass, the State, as did the Government in *Katz*, infringed a *legitimate expectation of privacy* that petitioner held").

21. See *id.* at 742.

22. See *Smith*, 442 U.S. at 744.

23. See *id.*

24. See *id.* ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and exposed that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed").

25. *Id.* at 748 (Brennan dissenting).

many has become a personal or professional necessity, he cannot help but accept the risk of surveillance"[26]. Justice Brennan added, "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative"[27]. Both allude to the risks related to the Third-Party Doctrine in the modern age. Technology has entrenched itself so deeply into people's lives that it has become a necessity. It is not simple to expect an individual to assume the risk of sharing information with a third party, when they have no other choice, and, at times, no awareness of the shared information.

2.2. *Third-Party Doctrine Stalls*

2.2.1. *Skepticism Over Third Party:* United States v. Jones

After decades of consistency, the Third-Party Doctrine came under scrutiny in the case *United States v. Jones*[28]. In *Jones*, Antoine Jones came under suspicion of drug trafficking[29]. The Government obtained a warrant to install a tracking device underneath his car which was parked in a public parking lot[30]. Over the next 28 days, the Government tracked the vehicle, collecting more than two thousand pages of data[31]. With the support of this data, Jones was charged with conspiracy to possess and distribute drugs[32]. Relying on the Third-Party Doctrine, the District Court suppressed the information obtained while the vehicle was parked in Jones's residence, but allowed everything else, reasoning that, since the roads on which Jones was traveling were public, he had no reasonable expectation of privacy[33]. The Court of Appeals disagreed and reversed the decision, finding that the Government's warrantless tracking of Jones's car was an intrusion of Fourth Amendment rights[34].

---

26. *Smith*, 442 U.S. at 750 (Marshall dissenting).
27. *Id.* (Brennan dissenting).
28. See *Jones*, 565 U.S. 400 (2012).
29. See *id*. at 402.
30. See *id.*
31. See *id*. at 403.
32. See *id.*
33. See *id*.
34. See *id*.

The Government appealed to the Supreme Court and argued that, although the information was not directly shared with a third party, it had been received through the use of the public road system, therefore, Jones had no reasonable expectation of privacy[35]. The Court disagreed, stating that, by attaching a device on Jones's vehicle, the Government invaded a constitutionally protected area[36] .

Although Justice Sotomayor ultimately agreed with the majority, she wrote in her prophetic concurring opinion that the Court should address the Third-Party Doctrine head-on[37]. She specifically referred to the impact of the doctrine on individuals in the modern age:

> People reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers ... I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year[38].

She suggested that a better solution to the problem would be to address the problem through the lens of *Katz*, according to which an individual has a reasonable expectation of privacy under the Fourth Amendment[39].

35. See *id.* at 410.

36. See *id.*

37. See *id.* at 417 (Sotomayor concurring: "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties").

38. *Id.*

39. See *id.* ("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").

2.2.2. *Winds of Change:* Carpenter v. United States

The wreck of the traditional notion of privacy, possibly caused by the appearance of digitalization in the modern world and influenced by the echoes of Jones, has driven the Supreme Court to a change in its attitude. In *Carpenter*, the landscape of police investigation had changed from the one in Jones, five years before. In April 2011, four men were arrested for a long string of armed robberies of cell phones in Ohio and Michigan[40]. The FBI managed to seize some of the members, turning them to their cause of capturing the rest[41]. The seized criminals quickly turned on Timothy Carpenter and his brother, providing the Government with their phone numbers[42]. The Government used the numbers to apply for court orders under the Stored Communications Act, in order to access cell phone records from Sprint and MetroPCS[43]. The first court order provided the Government with 152 days of cell-site location information records (CLSI), while the second supplied two more days of data[44]. Altogether, the Government had obtained 12,000 CSLI data pinpointing the location of an individual[45] and it was able to produce a detailed map that placed Carpenter near the robberies' sites[46]. Furthermore, they could theoretically go back five years and construct a detailed map of Carpenter's location throughout his life[47]. Carpenter was charged with six counts of robbery and carrying a firearm during a federal crime, and was convicted to more than 100 years of prison[48].

---

40. See *Carpenter*, 138 S. Ct. 2206, 2212 (2018).
41. See *id.*
42. See *id.*
43. See *id.* ("That statute, as amended in 1994, permits the Government to compel the disclosure of certain telecommunications records when it *offers specific and articulable facts showing that there are reasonable grounds to believe* that the records sought *are relevant and material to an ongoing criminal investigation*").
44. See *id.*
45. See *id.* ("Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI)").
46. See *id*. at 2213.
47. See *id*. at 2218.
48. See *id.* at 2213.

However, the Court determined that the Government had violated Carpenter's Fourth Amendment rights when they accessed CSLI data from the carriers, and in an unprecedented move[49], withdrew from the precedent of the Third-Party Doctrine and laid out a new balancing test, that could be used in similar circumstances[50]. *Carpenter* had a narrow view. The decision did not eliminate the possibility of obtaining location based on tower dumps, nor did it retreat from the established *Smith* and *Miller* decisions of obtaining information through banking records and cell phone records[51]. However, it established a balancing test for future cases to scrutinize warrantless police activity of an individual's private digital footprint[52].

The following sections will cover in detail the balancing test established in *Carpenter* and apply it to digital areas where it could serve as a gatekeeper to warrantless third-party information gathered by the Government. Perhaps, in the future, it may become a clear legal standard applicable to modern privacy conflicts.

3. *Analysis*

3.1. Carpenter *Balancing Test*

In what amounted to a severe misrepresentation by the Government, the assertion was that the Third-Party Doctrine applied to *Carpenter,* because cell phone location tracking data was similar to business records[53]. Justice Roberts, however, deduced an argument perpetuated by the Government, from *Miller* and *Smith* and established a balancing test. The application of this test could additionally be accounted for other pervasive technologies, which are currently being used by the Government to obtain individual data without any legal or official authorization[54].

49. See *id.* at 2220.
50. See *id.*
51. See *id.*
52. See *id.*
53. See *id.* at 2210.
54. See *id.*

Justice Roberts broke down the Third-Party Doctrine and applied it to Carpenter. Firstly, he assessed whether the individual had a reasonable or reduced expectation of privacy[55]. In determining so, the Court took two steps. The Court contrasted that in *Smith* and *Miller,* the shared information presented certain limitations, incomparable to those of *Carpenter*, "[t]here is a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected by wireless carriers today"[56]. Unlike banking records or a pen register, the wealth of CSLI allows the government a pervasive ability to trace a person's current and past location in a five-year time span with nearly perfect precision[57]. Furthermore, the information is time stamped, therefore, the level of pervasiveness increases as the Government is able to easily pinpoint their daily activity, be it a visit to religious institutions, their professional life, sexual associations, or other pursuits[58].

Secondly, Justice Roberts looked at whether voluntary exposure under the Third-Party Doctrine applies to CSLI. He reasoned that for the information to be truly voluntary, an individual had to have some choice in sharing the information. Cell phones have become so indispensable in everyday life, that they are almost required in the modern world, further diminishing one's options[59]. Even AT&T, who handsomely profits from the extensive use of their services, echoes a similar concern over the lack of genuine choice:

> *Smith* and *Miller* rested on the implications of a customer's knowing, affirmative provision of information to a third party and involved less extensive intrusions on personal privacy. Their rationales apply poorly to how individuals interact with one another and with information using modern digital devices ... a legal regime that forces individuals to choose between maintaining their privacy and participating in the emerging

55. See *id.*
56. *Id.*
57. See *id.* at 2210.
58. See *id.*
59. See *id.* at 2220.

> social, political, and economic world facilitated by the use of today's mobile devices or other location-based services[60].

Additionally, voluntariness connotes an affirmative act on the part of the user, however, in the case of CLSIs, the user makes no affirmative act aside from turning on the cell phone[61]. Once the user turns a phone on, any subsequent action (checking e-mail, phone calls or texts messages) generates a CLSI[62]. Thus, the user assumes no voluntary risk of sharing the data with a third party.

Putting it all together, the Court balanced the voluntary exposure of data with the reasonable expectation of privacy and found that the government had stepped on Carpenter's Fourth Amendment rights[63].

3.2. *Applying the Balancing Test*

3.2.1. *Tower Dumps*

Unfortunately for third-party denouncers, the narrow decision by the Court allowed the Third-Party Doctrine to advance mostly unabated[64]. In a convoluted move, the Court allowed tower dumps to continue[65]. Tower dumps are the big brother of CSLI. A CSLI is sought out when the government has a suspect in mind and is searching for their number in the midst of a haystack of numbers from a cell tower, at a particular time and location[66]. As in the case of Timothy

60. En Banc Brief of *Amicus Curiae* by Counsel for *Amicus Curiae* AT&T Mobility, LLC, not supporting either party, *United States of America v. Quartavious Davis,* 12–12928, *5–6 (11th Cir. filed November 17, 2014).

61. See *id.*

62. See *id.*

63. See *id.*

64. See *Carpenter*, 138 S. Ct. at 2220 ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or *tower dumps* ... We do not disturb the application of Smith and Miller or call into question conventional surveillance techniques and tools, such as security cameras").

65. See *id.*

66. See *Carpenter,* 138 S. Ct. at 2206 ("Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI)").

Carpenter, the collection of information in CSLIs might range from a few seconds to more than five years[67]. In contrast, in a tower dump, the government investigates criminal activities which take place at a certain location, at a particular time, and the suspect of which is unknown[68]. The timing aspect could vary between a few seconds and a few days, far shorter than CSLI, and yet no less intrusive[69].

Although tower dumps reveal less information about a particular individual, they are nonetheless highly intrusive. The provided information could be of little use to an investigation, taking into consideration the absence of identity of a suspect, but unlike CSLI, which can reveal somewhat about certain individuals, in the case of tower dumps, the Government is able to request the phone numbers and locations of every individual in an area, at a certain time – exponentially increasing the level of intrusiveness upon a multitude of individuals. For instance, in 2010, the FBI received more than 150,000 numbers in a single dump to determine the location of a suspect in a bank robbery, and there are more than 14,000 tower dump requests annually[70].

Further concerns follow the conclusion of the investigation, since there is little oversight on what happens to that information and its disposal, as certain governmental agencies have retained the information for many years[71]. The Government has revealed neither what measures are taken to notify those involved in the collection of information, nor whether any measures are in place to ensure that collection of data from unsuspected individuals is minimized[72].

Considering that CLSIs and tower dumps share a DNA, an application of the *Carpenter* balancing test should be straightforward. As

67. See *id.*

68. See Katie Hass, *Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions*, (ACLU, March 27, 2014), available at https://www.aclu.org/blog/national-security/privacy-and-surveillance/cell-tower-dumps-another-surveillance-technique (last visited April 26, 2020).

69. See Mason Kortz and Christopher Bavitz, *Cell Tower Dumps*, 63 Boston Bar Journal 27, 28 (2019).

70. See *id.*

71. See Ellen Nakashima, *Agencies collected data on Americans' cellphone use in thousands of 'tower dumps'*, (Washington Post, December 9, 2013), available at https://www.washingtonpost.com/world/national-security/agencies-collected-data-on-americans-cellphone-use-in-thousands-of-tower-dumps (last visited April 26, 2020).

72. *Id.*

to the aspect of pervasiveness, tower dumps provide the government with vast amounts of data on numerous individuals. Furthermore, this data, like CSLI, can be used to map out the daily activity of every single individual in the data set, which the government warrantlessly requested from various providers[73]. For the Court, such an intrusion on a known suspect was found to be too pervasive[74]. In the case of tower dumps, the data is of numerous unaware individuals whose privacy is intruded by the government to have an unknown needle in a haystack found.

It is argued that the data set considers a large number of unknown subscribers within a relatively small-time window[75]. However, taking into account that most, if not all, of these subscribers are innocent in whatever crime the government may be investigating, and these subscribers have not volunteered any information to third parties, it should be obvious that the *Carpenter* balancing test shall likewise apply to tower dumps[76]. These individuals did not assume the risk when they decided to use their phones, and for many they had no awareness of such level of intrusion[77]. As in the case of CSLI, these individuals simply want to engage in an inoffensive activity such as calling a beloved one, or connecting on social media (perhaps chuckling at a funny cat video). The information collected by subscribers is meant to serve the purpose of providing better cell service, and the participants are strung along with little choice in today's digital age. These individuals have no realistic alternative in the matter because all subscribers collect information through the use of their towers.

Lastly, to balance the voluntariness of tower dump data with the legitimate expectation of privacy others expect from that data, we would find that most of these individuals, as well as society, would have a legitimate expectation of privacy of the data.

---

73. See Kortz and Bavitz, *Cell Tower Dumps* 28 (cited in note 69).

74. See *Carpenter*, 138 S. Ct. at 2220.

75. See Amanda Regan, *Dumping the Probable Cause Requirement: Why the Supreme Court Should Decide Probable Cause is Not Necessary for Cell Tower Dumps*, 43 Hofstra L. Rev. 1189, 1217–1219 (2015).

76. See Katie Hass, *Cell Tower Dumps* (cited in note 68).

77. *Id.*

3.2.2. *Smart Homes*

Cicero wrote, "What is more sacred, what is more strongly guarded by every holy feeling, than a man's own home?"[78]. Words spoken centuries ago have permeated modern days in Western culture. We treat our home as a sacred place, which the Constitution under the Fourth Amendment has explicitly addressed as a place that should be "free from unreasonable governmental intrusion"[79]. Yet, as everything else, the digital revolution has penetrated our homes. We upgrade our "unintelligent" homes with Google Assistant, or the Amazon Echo, devices that now are able to control everything from turning on a TV to regulating our showers[80]. The devices are constantly in the working mode and listen to our instructions, with every syllable being recorded and preserved in servers, subsequently overseen by Google, Amazon, and other third parties[81]. They may even indivertibly catch us in the process of what the government may later construe as criminal conduct.

One evening, James A. Bates and his co-workers decided to watch a football game and have a drink at Bates's home[82]. The co-workers stayed for the night, and in the morning, one of them was found drowned in the bathtub[83]. Law enforcement officers found blood and broken bottles around the bathtub, and the medical examiner concluded the case as homicide[84]. Law enforcement immediately seized Bates's electronics and obtained a search warrant directing Amazon to provide vast amounts of information in the hopes of finding among the records any hint to struggle or argument that led to the co-worker's

78. Marcus Tullius Cicero, *Ad Pontifices,* XLI, 109.

79. U.S. Const. Amend. IV.

80. See Jay Stanley, *The Privacy Threat From Always-On Microphones Like Amazon Echo* (ACLU, January 13, 2017), available at https://www.aclu.org/blog/privacy-technology/privacy-threat-always-microphones-amazon-echo (last visited April 26, 2020).

81. *Id.*

82. See Amy B. Wang, *Police land Amazon Echo data in quest to solve murder* (Chicago Tribune, March 9, 2017), available at https://www.chicagotribune.com/business/blue-sky/ct-amazon-echo-murder-wp-bsi-20170309-story.html (last visited April 26, 2020).

83. *Id.*

84. *Id.*

death[85]. Law enforcement has also obtained data from Bates's smart water meter, by showing a simple probable cause, in attempts to uncover extensive use of water to wash away blood[86]. Amazon contested the search in their motion stating that the request "would chill users' exercise of their free speech rights to seek, receive, and review information in the privacy of their own homes"[87]. They further indicated that the amount of requested information goes beyond what a mere document could provide[88].

From Bates's point of view, at no point could he have contested his privacy concern over the data held by Amazon and seized by law enforcement. His privacy concerns – in his own home – were disregarded and the fight ultimately raged between law enforcement and third parties over the data[89]. Although Bates eventually consented to the search, and law enforcement later dropped the charges, the invasion into Bates's privacy painted a bleak picture of the modern-day deterioration of privacy – an invasion of one's castle[90]. Bates's attorney stated as follows: "[y]ou have an expectation of privacy in your home, and I have a big problem that law enforcement can use the technology that advances our quality of life against us"[91].

Taking the previous event into account, one can easily see that the Court needs to take a serious look at Third-Party Doctrine, apply the *Carpenter* balancing test as a legal standard to smart home devices, and extend a reasonable expectation of privacy to such data. Under the *Carpenter* balancing test, we would first look at whether someone would have a legitimate or reduced expectation of privacy in the

85. *Id.*

86. See Amy B. Wang, *Police land Amazon Echo data in quest to solve murder* (cited in note 83).

87. Morgan M. Wiener, *Digital Evidence and Privacy: Can you ask Alexa if mom's incapacitated?* (Holland & Heart LLP, March 1, 2017), available at http://www.lexology.com/library/detail (last visited April 26, 2020).

88. *Id.*

89. *Id.*

90. See Amy B. Wang, *Police land Amazon Echo data in quest to solve murder* (cited in note 82).

91. Eric Boughman, et al., *"Alexa, Do You Have Rights?": Legal Issues Posed by Voice-Controlled Devices and the Data They Create* (American Bar Association, July 20, 2017), available at https://www.americanbar.org/groups/business_law/publications/blt/2017/07/05_boughman (last visited April 26, 2020).

information shared in their own homes. When addressing one's legitimate expectation of privacy, an observation could indicate the limitations one expects when sharing information in their own homes, and the pervasiveness one can experience when the Government obtains such information – with only probable cause if necessary.

The Fourth Amendment has always presented a strict limitation when one's property is invaded; and a firm line is drawn at the door of the home[92]. Even if a person is to share that data with some third party, that information should undergo the strictest scrutiny and a person should have a legitimate expectation of privacy in that data. In Bates's case, an absent search warrant left no ground for law enforcement to obtain the data from third parties; the Government obtaining the data without a warrant is absolutely pervasive. What purpose would the Fourth Amendment serve if the Government's intrusion in the homes and obtained data on the ground of being shared with third parties were to be confronted with the idle reaction? When at home, people are in the most vulnerable, relaxed and intimate state; a great level of privacy is expected in the abode from intruders. The information shared with third parties carries the same insecurities when intruded upon, and at times the same level of intimacy. A person has a legitimate expectation of privacy in that data, and should be the one deciding whether the data is necessary to be handed to authorities.

The second element to consider from the *Carpenter* balancing test is whether there is some voluntary exposure in sharing data from devices in one's own home. What transpired in Bates's home that evening is something that may never be known. However, there was no indication that Bates took a voluntary risk by bringing an Amazon Echo into his own home[93]. When individuals purchase the devices, they have no intention of sharing their voice recordings with an outside party. Instead, they are simply looking for simplification of their daily routines – playing music, turning on the TV, obtaining an innocuous factoid from the internet. Bates behaved similarly. He took

92. See *Payton v. New York*, 445 U.S. 573, 590 (1980) ("In terms that apply equally to seizures of property and to seizures of persons, the Fourth Amendment has drawn a firm line at the entrance to the house").

93. See Morgan M. Wiener, *Digital Evidence and Privacy: Can you ask Alexa if mom's incapacitated?* (Holland & Heart LLP, March 1, 2017), available at http://www.lexology.com/library/detail (last visited April 26, 2020).

no affirmative act when using his Amazon Echo, aside from deciding to listen to some music[94].

Finally, if the balance is struck in Bates's voluntary exposure of the data with the legitimate expectation of privacy, it would be found that Bates had a legitimate expectation of privacy in the data shared in his home.

4. *Conclusion*

Privacy has always been a cornerstone of American identity. For centuries, the Fourth Amendment has stood as guardian at the gate armed with the following words:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized[95].

Yet, the rise of the Third-Party Doctrine certainly proved a strong adversary to this guardian. It carved exceptions into the body of the Fourth Amendment and supplied the Government with the necessary tools to defeat it. It exposed people to insecurity in their own houses through devices such as Amazon Echo. The documents and belongings that now reside in digital format on the cloud, can be accessed by the Government without warrants upon the showing of probable cause. Fortunately, the Amendment withstands today, and yet, it requires reinvigoration. Just as *Katz* complemented the Fourth Amendment with the precious armor of reasonable expectation of privacy, the same must be done with the shield of *Carpenter*[96].

Firstly, it must be inquired whether the individual has a reasonable or reduced expectation of privacy by assessing the level of

94. *Id.*
95. U.S. Const. Amend. IV.
96. See *Katz*, 389 U.S. at 360.

pervasiveness of the Government in the individual's digital data[97]. Secondly, it shall be considered whether voluntary exposure under the Third-Party Doctrine applies to the digital shared data by assessing whether the individual has some choice in sharing the information, by assuming some risk when doing so[98]. Lastly, the legitimate expectation of privacy is weighed against the voluntariness of the shared information, and a decision is made as to whether the information could be outside the purview of an individual's legitimate expectation of privacy[99]. It can therefore be assumed that the Fourth Amendment has been fortified and reinvigorated in the digital age and beyond.

97. See *Carpenter*, 138 S. Ct. at 2210.
98. *Id.* at 2220.
99. *Id.*