"ALEXA, ARE YOU LISTENING?" USING *CARPENTER* AND TRADITIONAL PROPERTY-BASED FOURTH AMENDMENT ANALYSES TO DETERMINE HOW VOICE ASSISTANT DATA CAN BE PROTECTED UNDER THE FOURTH AMENDMENT

Jessica D. Cox*

I. INTRODUCTION

When the IBM Shoebox debuted as the first digital speech recognition tool in 1961, IBM probably had no idea that it had created a technological earthquake that would eventually result in a wave of technological advancements and adoptions that would overtake the United States like a tsunami by 2018.[1] The first smart speakers—the Amazon Alexa and Echo—debuted in November of 2014,[2] and since that time, "Alexa" has become a household name with thirty million smart speakers sold globally in 2017 and sixty million projected to be sold in 2018.[3] The growing popularity of smart speakers and other voice assistants has begun to raise privacy concerns as unsuspecting consumers realize the new gadget they

* Juris Doctor Candidate, Oklahoma City University School of Law, 2020; Master of Business Administration, University of Oklahoma, 2003. Thank you to Professor Mark Blitz for his patience and guidance during the writing process. Thank you also to my family and friends for believing in me. Special thanks to my loving husband, Terry, who selflessly encourages and enables me to pursue my dreams. Finally, thanks to my children, Koribella, Howard, and Maximus, whose hugs and kisses make the world a better place.

1. Ava Mutchler, *A Timeline of Voice Assistant and Smart Speaker Technology from 1961 to today*, VOICEBOT.AI (Mar. 28, 2018, 2:56 PM), https://voicebot.ai/2018/03/28/timeline-voice-assistant-smart-speaker-technology-1961-today/ [https://perma.cc/UP85-WFGY].

2. *Id.*

3. Bernard Marr, *Machine Learning in Practice: How Does Amazon's Alexa Really Work?*, FORBES (Oct. 5, 2018, 12:01 AM), https://www.forbes.com/sites/bernardmarr/2018/10/05/how-does-amazons-alexa-really-work/#6e2df3011937 [https://perma.cc/TV43-ZVXS].

brought into their home could be secretly recording intimate conversations and sharing those conversations with other people without their knowledge or permission.[4] Additionally, while manufacturers of smart speakers deny that consumers are unknowingly recorded,[5] some law enforcement officials believe that these potential recordings should be considered an additional means of acquiring evidence in a criminal investigation.[6]

Evident by the legal concerns arising from cases like *Arkansas v. Bates* and *State v. Verrill*,[7] it is critical that our laws evolve in lockstep with technology to maintain the protections our Constitution provides citizens.[8] When *Carpenter v. United States*[9] was granted certiorari, scholars hoped for clarity concerning application of the Fourth Amendment privacy protections to unavoidable digital data[10] held by third parties.[11] Unfortunately, the Court's decision in *Carpenter* is intentionally narrow and provides little general guidance for how unavoidable digital data should be treated with respect to the Fourth Amendment and the third-party doctrine.[12] Nevertheless, this Note shows how the Court's reasoning

4. Peter Newman, *Echo's Recent Eavesdropping Incident Could Undermine Amazon and the Smart Speaker Market as a Whole*, BUSINESS INSIDER (May 29, 2018, 10:59 AM), https://www.businessinsider.com/amazon-echo-eavesdropping-incident-undermining-smart-speaker-market-2018-5 [https://perma.cc/K5UZ-N9BB].

5. *Alexa and Alexa Device FAQs*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 [https://perma.cc/NAQ2-S3GB] (last visited Mar. 12, 2019).

6. *See* Elliott C. McLaughlin, *Suspect OKs Amazon to Hand Over Echo Recordings in Murder Case*, CNN, https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html [https://perma.cc/4FM8-KQGS] (last visited Mar. 12, 2019); Debra Cassens Weiss, *Judge Orders Amazon to Provide Echo Recordings in Double Homicide Case*, ABA JOURNAL (Nov. 12, 2018, 2:48 PM), http://www.abajournal.com/news/article/judge_orders_amazon_to_provide_echo_recordings_in_double_homicide_case/ [https://perma.cc/CVH8-NXXD].

7. *Id.*

8. *See* Kyllo v. United States, 533 U.S. 27, 33-35 (2001).

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

10. The term *unavoidable digital data* refers to classes of data that are similar in characteristics to the cell-site location information (CSLI) described in *Carpenter* as having a "deeply revealing nature . . . [with] depth, breath, and comprehensive reach, and . . . inescapable and automatic nature of . . . collection." *Id*. at 2223.

11. *See*, *e.g*., Daniel Solove, *10 Reasons Why the Fourth Amendment Third Party Doctrine Should Be Overruled in* Carpenter v. US, TEACHPRIVACY (Nov. 28, 2017), https://teachprivacy.com/carpenter-v-us-10-reasons-fourth-amendment-third-party-doctrine-overruled/ [https://perma.cc/2QJ6-6D32].

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

from *Carpenter* can be applied to data collected by voice assistants and discusses why that might not be the best approach. Recognizing that the common-law property-based principles that dominated the Fourth Amendment jurisprudence prior to *Katz v. United States* remain a viable option for protecting citizens' rights, this Note will also propose a standard by which smart speaker data can be analyzed under that traditional property-based Fourth Amendment jurisprudence without the need for the doctrines relied on in *Carpenter*.

Part I will briefly review relevant Fourth Amendment jurisprudence and the third-party doctrine as well as describe smart speakers and the data they collect. Part II will lay out two possible doctrines under which smart speaker data protections could be analyzed. First, by using a *Carpenter*-style exception to the third-party doctrine; second, by applying traditional property-based Fourth Amendment considerations. Part III will analyze the nature of smart speaker data, apply the two proposed doctrines to that data, and ultimately explain how traditional Fourth Amendment common-law property considerations can be applied to smart speaker data to provide sufficient privacy protections without relying on the *Katz* "reasonable-expectation-of-privacy" doctrine.

II. SETTING THE STAGE

A. Evolution of Fourth Amendment Protections

1. Defining a Search – When Has a Search Occurred?

The Fourth Amendment protects the right of a person "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[13] The purpose of the Amendment is not to provide a "general constitutional 'right to privacy,'"[14] but rather to prevent the types of general searches frequently employed by the colonial-age "British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[15] Therefore, a proper inquiry into the application of the Fourth Amendment begins by asking whether a search occurred. A traditional Fourth Amendment application then begins to explore whether

13. U.S. CONST. amend. IV.

14. *Carpenter*, 138 S. Ct. at 2240 (Thomas J., dissenting) (quoting Katz v. United States, 389 U.S. 347, 350 (1967)).

15. *Id*. at 2213.

the person had a common-law property interest that was violated when the Government obtained the information.[16] This common-law property interest was further expanded in *Silverman v. United States*[17] when the Court based its decision "upon the reality of an actual intrusion into a constitutionally protected area."[18] Additionally, the *Silverman* holding implicitly expanded Fourth Amendment protections to "the overhearing of verbal statements as well as against the more traditional seizure of 'papers and effects.'"[19] However, it is not until *Berger v. New York* that the Court "brings wiretapping and other electronic eavesdropping fully within the purview of the Fourth Amendment"[20] by silently—but effectively—overruling nearly forty years' worth of cases that previously held wiretapping without a physical trespass and authorized by a warrant issued with probable cause does not violate the Constitution.[21]

Although the protection of conversations was a significant evolution of Fourth Amendment jurisprudence, the biggest expansion of Fourth Amendment protections resulted from the *Katz*[22] "reasonable-expectation-of-privacy" test born out of Justice Harlan's concurrence.[23] In *Katz*, the Court held that "the Fourth Amendment protects people, not places" and, consequently, certain "expectations of privacy as well."[24] This holding resulted in the establishment of a two-pronged, objective and subjective, inquiry to determine if a constitutionally protected search has occurred. First, a person must demonstrate a genuine expectation of privacy in the information in question and, second, the expectation must be one that society is willing to recognize as reasonable.[25] *Katz* further established that

16. *Id.*

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

18. *Id.* at 512.

19. Berger v. New York, 388 U.S. 41, 52 (1967) (quoting Wong Sun v. United States, 371 U.S. 471 (1963)).

20. *Id.* at 64 (Douglas, J., concurring).

21. *See* Olmstead v. United States, 277 U.S. 438, 468 (1928) (holding that obtaining evidence by wiretapping does not violate the Constitution without a unlawful entry into a home); Goldman v. United States, 316 U.S. 129, 134 (1942) (holding that use of a detectaphone to hear private conversations in the next room did not violate the Constitution without a physical trespass); On Lee v. United States, 343 U.S. 747, 751 (1952) (finding since no trespass was committed when recording a conversation no violation of the Constitution occurred).

22. Katz v. United States, 389 U.S. 347 (1967).

23. *Id.* at 360 (Harlan, J., concurring).

24. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (quoting *Katz*, 389 U.S. at 351 (1967)).

25. Smith v. Maryland, 442 U.S. 735, 740 (1979).

"reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[26] The Court in *Kyllo v. United States*[27] expanded on this holding regarding electronic invasion to find that a constitutionally protected search occurred when police used technology "not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion."[28]

While the reasonable-expectation-of-privacy test has come under significant scrutiny,[29] it continues to be relied on and may even overshadow the traditional property-based understanding that "if a house, paper or effect [is] *yours* under law" then Fourth Amendment protections apply.[30] In fact, the Court in *United States v. Jones* felt it necessary to reiterate that "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test"[31] and that "[w]hen 'the Government obtains information by physically intruding' on persons, houses, papers, or effects, 'a search within the original meaning of the Fourth Amendment' has 'undoubtedly occurred.'"[32] Likewise, in *Florida v. Jardines*,[33] the Court reminded us that when the knowledge gained by the officers is a direct result of a physical property intrusion, "we need not decide whether the officers' investigation . . . violated . . . [an] expectation of privacy under *Katz*."[34]

Conversely, a search cannot occur if the individual does not have a recognized property interest or a reasonable expectation of privacy that has been violated. Furthermore, the Court has found that a person cannot have a reasonable expectation of privacy if he shares information with a third party, which in turn shares with the government, even if he thought that person would keep the information secret.[35] Applying this principle that Fourth Amendment protections are lost when information is disclosed to a third party, the Court held that a person retains no legitimate expectation of privacy in papers shared with a personal accountant,[36]

26. *Katz*, 389 U.S. at 362.
27. Kyllo v. United States, 533 U.S. 27 (2001).
28. *Id.* at 40.
29. *Carpenter*, 138 S. Ct. at 2214 n.1.
30. *Id.* at 2268.
31. United States v. Jones, 565 U.S. 400, 409 (2012).
32. Florida v. Jardines, 569 U.S. 1, 5 (2013) (quoting *Jones*, 565 U.S. at 406 n.3).
33. *Jardines*, 569 U.S. at 1.
34. *Id.* at 11.
35. United States v. Miller, 425 U.S. 435, 443 (1976).
36. Couch v. United States, 409 U.S. 322, 335-36 (1973).

personal bank records disclosed to a bank,[37] or dialed phone numbers voluntarily conveyed to the phone company.[38] This doctrine, known as the third-party doctrine, outlines an area of law where Fourth Amendment protections simply do not apply.[39]

However, the advancement of technology makes applying the third-party doctrine difficult because more people are entrusting their communications to third parties. In *United States v. Warshak*, the Court of Appeals for the Sixth Circuit addresses the technological advancement of email communications and grapples specifically with the issue of "whether the government is permitted to request that a commercial ISP turn over the contents of a subscriber's emails without triggering the machinery of the Fourth Amendment."[40] The Court begins its analysis by restating two "bedrock principles" of the Fourth Amendment. "First . . . information . . . passed through a communications network is a paramount Fourth Amendment consideration. . . . Second, the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[41] It continues by analogizing email communications to traditional forms of communication which have been mostly supplanted by emails, such as phone calls and letters. *Warshak* determined that emails could not be afforded a lesser level of protection under the Fourth Amendment than its communication predecessors.[42]

Additionally, *Warshak* established that "the mere *ability* [or right for] a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy."[43] Once again, the Court relied on its analogy to the telephonic communications, but also compared it to the privacy rights of hotel patrons and residential tenants which are not spoiled by others having a right of access to refresh linens or fix a leaky faucet.[44] Finally, the Court distinguished *Warshak* from *Miller* stating that the documents in question in *Miller* were not "confidential communications" sent through an

37. *Miller*, 425 U.S. at 442.
38. Smith v. Maryland, 442 U.S. 735, 745 (1979).
39. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).
40. United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010), *reh'g denied*, 2011 U.S. App. LEXIS 5007.
41. *Id.* at 285-86.
42. *Id.*
43. *Id.* at 286-87.
44. *Id.* at 287.

intermediary, but rather business records conveyed to the bank for the purpose of conducting regular business.[45] Thus, it found that "*Miller* [was] not controlling."[46] Similarly, as this Note will discuss in more detail in Part II, the United States Supreme Court declined to extend the previously established third-party doctrine principles to cell phone location records held by a third party in *Carpenter v. United States*.[47]

2. Recognized Exceptions to the Protections of the Fourth Amendment

While the Fourth Amendment does provide protections, it is only against *unreasonable* searches and seizures. Therefore, an intrusion may not violate the Constitution if the government first obtains a warrant with probable cause pursuant to the Warrant Clause of the Fourth Amendment.[48] Additionally, it is well-recognized that "when a person is lawfully arrested, the police have the right, without a search warrant, to make a contemporaneous search of the person of the accused for weapons or for the fruits of or implements used to commit the crime."[49] The search may include things that are within the accused's span of control and the location of the arrest depending on the circumstances surrounding the arrest but only within a time and space not too remote from that of the arrest.[50] The constitutionality of these warrantless searches hinges on the necessity to protect the officer from hidden weapons and to prevent the escaping of the arrestee.[51] Thus, they are considered "reasonable" under the Fourth Amendment.

This exception to the Warrant Clause was further defined by the Court in *Terry v. Ohio*.[52] In *Terry*, the Court held that a police officer, with reasonable suspicion that a suspect is armed, is permitted to conduct a limited search of a suspect's outer clothing to verify the presence or absence of a weapon even before an arrest occurs, and that search will be held reasonable under the Fourth Amendment.[53] Once again, the purpose for this exception is to allow the officer to ensure her own and others'

45. *Id*. at 287-88.
46. *Id.*
47. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
48. Terry v. Ohio, 392 U.S. 1, 20 (1968).
49. Preston v. United States, 376 U.S. 364, 367 (1964).
50. *Id.*
51. *Id.*
52. *Terry*, 392 U.S. at 1.
53. *Id.* at 29-31.

immediate personal security when performing her duties by exercising appropriate discretion based on her professional training and knowledge.[54] However, in *Riley v. California*,[55] the Court was faced with reconciling these warrantless searches with the age of technology and the proliferation of the modern cell phone in our society.[56] While the Government contended that a cell phone is no different than any other object that a person may carry and would be searched incident to an arrest, the Court recognized that the cell phone is a "minicomputer" made up of a number of previously independent machines or items.[57] Given the immense invasion of privacy resulting from a search of cell phone contents and the lack of immediate government necessity, *Riley* declared that a search of a cell phone, even if seized incident to an arrest, requires a warrant.[58]

B. Voice Assistants Defined

1. What Are They and What Do They Do?

The voice recognition technology—first introduced in 1961 with IBM's Shoebox recognizing just sixteen words[59]—has blossomed into an entire voice assistant industry in which software developers are using artificial intelligence coupled with machine learning to improve voice recognition. The technology has progressed significantly since Shoebox's time, and now "Google speech . . . recognizes 19 out of 20 words [that] it hears."[60] Voice assistants—like Amazon Alexa, Google Assistant, and Microsoft Cortana—can now respond to users who verbally interact with smart devices such as speakers, televisions, and cell phones.[61] Each smart device must be equipped with a microphone, speaker, and internet connection to access a voice assistant.[62] Whenever a user asks a question

54. *Id.*
55. Riley v. Carpenter, 134 S. Ct. 2473 (2014).
56. *Id.* at 2485.
57. *Id.* at 2488-89.
58. *Id.* at 2493.
59. Mutchler, *supra* note 1.
60. Marr, *supra* note 3.
61. Joe Svetlik, *Alexa, Cortana, Google Assistant: What Are Voice Assistants and How Do They Work?*, BT (Feb. 20, 2019, 6:38 PM), http://home.bt.com/tech-gadgets/internet/broadband/alexa-cortana-google-assistant-what-are-voice-assistants-and-how-do-they-work-11364211957737 [https://perma.cc/4Y7V-26GY].
62. *Alexa Voice Services*, AMAZON, https://developer.amazon.com/alexa-voice-service [https://perma.cc/Q8ND-ZYN9] (last visited Mar. 13, 2019).

of or makes a command to a device equipped with a voice assistant, the device creates a recording of the question or command and sends it across the internet to the Cloud where the request is decoded using voice assistant software, and then an audio response is returned through the speaker in the device.[63] Using this basic communication model, a voice assistant enabled device can provide services such as answering simple questions, setting a timer, checking the weather, editing a shopping or to-do list, and even purchasing something at the user's verbal command or request. Developers are working now to incorporate internet connectivity to more simple devices so that voice assistants can provide additional services like locking doors and adjusting lighting with a goal of a user being able to control every aspect of her home by verbally interacting with a voice assistant enabled device.[64]

To improve the accuracy of the voice assistant responses that are relayed to consumers, manufacturers like Amazon use consumer data (interactions with smart speakers) to fuel "machine learning"[65] which enables Alexa to "train [its] speech recognition and natural language understanding systems."[66] This means that Amazon, Google, and Microsoft are keeping copies of all those snippets of data that are being sent to the Cloud by every user and using those recordings to make their programs work better.[67] Further, Amazon is using the consumers' data to improve other services that it offers.[68] Each of the recordings is associated with a specific consumer's account, and Amazon allows consumers to log in to their account to review recordings, delete recordings, and indicate if and how Amazon is allowed to use the recordings.[69] Amazon insists that it is not recording all the time and that only the necessary data is stored in the Cloud,[70] but this model of service requires either a button to be pressed

63. Marr, *supra* note 3.

64. *Alexa for Device Makers*, AMAZON, https://developer.amazon.com/alexa/devices?&sc_category=Owned&sc_channel=WB&sc_publisher=Website&sc_content=Content&sc_detail=SubNav&sc_funnel=Visit&sc_country=US&sc_medium=Owned_WB_Website_Content_SubNav_Visit_US_SiteVisitors&sc_segment=SiteVisitors [https://perma.cc/G3G4-N3CC] (last visited Mar. 13, 2019).

65. Marr, *supra* note 3.

66. *Alexa and Alexa Device FAQs*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 [https://perma.cc/6A6J-YPY4] (last visited Mar. 12, 2019).

67. *Id.*

68. *Id.*

69. *Id.*

70. *Id.*

to "wake" the recording device or the microphone to be always on and listening for a "wake-up word" or phrase.[71]

The always-on microphone has presented the biggest privacy issues for voice assistant enabled devices.[72] Several incidents involving privacy breaches have already occurred: Google Home Mini was found to be recording when the wake up word had not been used;[73] Amazon's Alexa recorded a family's conversation and sent it to a contact;[74] and both Alexa and Google have been triggered by either radio or television commercials.[75] Although the device manufacturers in every instance have responded by updating their code to address the concerns,[76] the opportunity for hackers and mischief-makers will never be completely removed.[77] Nevertheless, consumers are not deterred from filling their homes with voice-based artificial intelligence devices, and the number of homes with these devices in the United States is expected to increase as more manufacturers begin to introduce products.[78]

Although voice assistants are on many devices, the most commonly used ones are smart speakers, with Amazon's Echo leading the market in unit sales in 2018.[79] This Note will focus primarily on the privacy concerns around smart speakers, but do note that these same concerns will apply to any connected device that is using the voice assistant services and adding to the recordings and other data that are kept by the services.

71. Candid Wueest, *Everything You Need to Know About the Security of Voice-Activated Smart Speakers*, SYMANTEC (Nov. 20, 2017), https://www.symantec.com/blogs/threat-intelligence/security-voice-activated-smart-speakers [https://perma.cc/VUK2-D53Q].

72. *Id.*

73. *Id.*

74. Newman, *supra* note 4.

75. Wueest, *supra* note 71.

76. Chris Smith, *Radio Broadcast Caused Amazon Echo to Reset User's Home Thermostat*, TRUSTED REVIEWS (Mar. 11, 2016, 6:54 PM), https://www.trustedreviews.com/news/radio-broadcast-caused-amazon-echo-to-reset-user-s-home-thermostat-2939444#8IPemaDJPAz0xGKd.99 [https://perma.cc/HUT9-QMZN].

77. Wueest, *supra* note 71.

78. George Anders, *Alexa, Understand Me*, MIT TECHNOLOGY REVIEW (Aug. 9, 2017), https://www.technologyreview.com/s/608571/alexa-understand-me/ [https://perma.cc/5UGP-ETZE].

79. *Id.*

2. Current Cases Concerning Smart Speakers

While Amazon is using its customers' recordings to improve its products, law enforcement has different ideas about how to use these seemingly benign recordings and household data. The police department in Bentonville, Arkansas, believed that Amazon Echo data could provide insight into what happened one early morning in November 2015 in the Bates' home that resulted in the death of a man.[80] The officers served a search warrant on Amazon stating that "Amazon.com is in possession of records related to a homicide investigation . . . namely electronic data in the form of audio recordings, transcribed records, or other text records related to the communications and transactions between an Amazon Echo device . . . and Amazon.com's servers and other computer hardware."[81] The warrant made national news because Amazon resisted complying by claiming the warrant was overbroad and violative of the First Amendment. However, Amazon ended the legal battle in April 2017 when James Bates consented to the release of the recordings from his account.[82] The case was later dropped when prosecutors determined that the available evidence could not rule out other reasons for the man's death.[83]

The *Bates* case is believed to be the first of its kind in which law enforcement officials have sought recordings from an Amazon smart speaker,[84] but it was not the last. In January 2017, when two women were found dead in a Farmington, New Hampshire, home, prosecutors once again looked to Amazon to turn over recordings and other data from the Amazon Echo that was in the kitchen of the home believing that it could have been activated during the murder and something meaningful might have been recorded.[85] In November 2018, a county judge ordered Amazon to release the data granting a "motion to search in lieu of a search warrant," but Amazon is still resisting.[86] Only time will tell what other cases will

80. McLaughlin, *supra* note 6.

81. Memorandum of Law in Support of Amazon's Motion to Quash Search Warrant Exhibit A-2, at 1, Arkansas v. Bates, No. CR-2016-370-2 (Ark. Cir. Ct. Feb. 17, 2017) (Search Warrant), https://www.courthousenews.com/wp-content/uploads/2017/02/EchoQuash.pdf [https://perma.cc/9956-76TY].

82. McLaughlin, *supra* note 6.

83. Cassens Weiss, *supra* note 6.

84. McLaughlin, *supra* note 6.

85. Cassens Weiss, *supra* note 6.

86. Lyle Frink, *Alexa! You're the Witness … Who Killed Her?* (Nov. 20, 2018), https://blog.avira.com/alexa-youre-the-witness-who-killed-her/ [https://perma.cc/KTT4-ETQZ].

ripen as the proliferation of smart speakers continues,[87] and it is critical that citizens' Fourth Amendment rights are not allowed to be eroded by this emerging technology.[88]

3. Other Privacy Concerns Around Smart Speakers

Privacy risks associated with smart speakers employing voice assistants are plentiful.[89] California is the first state to recognize and do something about the burgeoning concerns around the lack of cybersecurity features included by manufacturers of internet-connected devices.[90] These new regulations require manufacturers of internet-connected devices (like smart speakers) to build them with cybersecurity features that will make it more difficult for hackers to access the millions of internet-connected devices.[91] This is good news when you consider features like the Amazon Echo's "drop-in," which allows a user to access a device remotely and begin listening in like an intercom.[92] If a hacker—or the government—gained access to "drop-in" to your device and listen in on what is happening in your home without your knowledge, then any amount of privacy protections for the stored recordings are unnecessary because an entity could hear in real time all of the conversations happening in your home within "earshot" of your smart speaker. This type of intrusion would be akin to wiretapping. Given the increasing opportunity for individuals' Fourth Amendment rights to be violated by government officials seeking to supplement their investigative efforts, it is critical that we have a standard for when Fourth Amendment protections should apply to the smart speaker data.

87. *Id.*
88. Kyllo v. United States, 533 U.S. 27, 34 (2001).
89. Wueest, *supra* note 71.
90. Jason Tashea, *California Imposes New Regulations on 'Internet of Things' Devices*, ABA JOURNAL (Dec. 10, 2018, 7:00 AM), http://www.abajournal.com/news/article/new_california_imposes_regulations_on_the_internet_of_things/ [https://perma.cc/KQ8J-44LA].
91. *Id.*
92. Wueest, *supra* note 71.

III. TWO WAYS TO ANALYZE SMART SPEAKER DATA

A. Carpenter *Majority Uses Reasonable-Expectation-of-Privacy Test*

When the Court granted certiorari to hear *Carpenter v. United States*,[93] many people were eagerly awaiting the decision that would follow to see how it would move Fourth Amendment jurisprudence into the digital age.[94] However, instead of addressing the larger question of how the Fourth Amendment applies to unavoidable digital data generally, the Court in *Carpenter* specifically examined if a Fourth Amendment search occurs when the Government obtains comprehensive cell-site location information (CSLI) from a person's cell phone provider.[95] This narrow analysis leaves many questions unanswered and creates some uncertainty as to how other digital data should be regarded. This Note seeks to use the analyses in the majority and dissents of *Carpenter*, which focus solely on CSLI, to provide a standard that could be applied to smart speaker data and potentially other unavoidable digital data as well.

Because the *Carpenter* opinion focuses on CSLI, it is important to understand how this data is collected. A "cell site" is a set of radio antenna that can be mounted on a tower, light post, or building that allows cell phones to connect and perform functions.[96] CSLI, a time-stamped record, is generated each time a cell phone connects with a cell site, which can be multiple times per minute because cell phones are constantly scanning their environments for the best signal.[97] Anyone who carries a cell phone is generating CSLI simply by turning it on. As the number of people using cell phones increases, wireless carriers are adding more cell sites to handle the increased traffic resulting in more accurate location information since the best signal will typically be the closest cell site.[98] Because carriers are tracking not only CSLI from phone calls but also text messages and data connections, "modern cell phones are generat[ing] vast amounts of increasingly precise CSLI."[99] Carriers collect and store CSLI data for their own purposes such as evaluating their networks, billing users, and even

93. Carpenter v. United States, 138 S. Ct. 2206 (2018).
94. *See, e.g.*, Solove, *supra* note 11.
95. *Carpenter*, 138 S. Ct. at 2211.
96. *Id.*
97. *Id.*
98. *Id.*
99. *Id.* at 2212.

selling summarized data to data brokers.[100]

It is this detailed location data that helped put Timothy Carpenter in prison for a long time.[101] He became a suspect in a string of Radio Shack and T-Mobile burglaries in Michigan and Ohio in 2011 when a suspect in custody for robbery pegged Carpenter as one of his fifteen accomplices.[102] Based on that information, prosecutors sought to obtain cell phone records of Carpenter and some other suspects with court orders issued pursuant to the Stored Communications Act.[103] "That statute . . . 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.'"[104] The Court issued two court orders: one seeking one hundred fifty-two days of CSLI from Metro PCS and one for seven days from Sprint. These orders produced a catalog of Carpenter's movements with 12,898 location points.[105]

Although, Carpenter had attempted to suppress the CSLI data arguing that it violated his Fourth Amendment rights because it was obtained without a warrant subject to probable cause, the district court held that the data was admissible.[106] The FBI's expert witness used this data to demonstrate that Carpenter was "right where the . . . robbery was at the exact time of the robbery."[107] Carpenter was convicted of several charges and received a sentence of more than 100 years in prison.[108] On appeal, the Sixth Circuit affirmed the conviction by relying on the third-party doctrine holding that "Carpenter lacked a reasonable expectation of privacy in the location information . . . because he had shared that information with his wireless carriers."[109]

The Court recognized this inquiry as a novel issue of law that lies at the intersection of two established areas of law: the first being "a person's expectation of privacy in his physical location and movements" and the second being the "line between what a person keeps to himself and what

100. *Id.*
101. *Id*. at 2206.
102. *Id.* at 2212.
103. *Id.*
104. *Id.* (quoting 18 U.S.C. 2703(d) (2015)).
105. *Carpenter*, 138 S. Ct. at 2212.
106. *Id.*
107. *Id.* at 2212-13.
108. *Id.* at 2213.
109. *Id.*

he shares with others*"*—the third-party doctrine.[110] Then, the Court began the analysis by using the two-prong subjective and objective reasonable-expectation-of-privacy test from *Katz* as it applies to a person*'*s physical movements. It stated that, in *Jones*, the Court recognized both that a person has an expectation of privacy in her own movements and that society recognizes that law enforcement could not possibly secretly follow and catalog an individual*'*s every movement.[111] Based on these established privacy expectations, the Court concluded that allowing government access to cell-site records goes against these expectations and that *"*[a]lthough such records are generated for commercial purposes,*"* Carpenter still maintains an expectation of privacy in his movements.[112]

Furthermore, the Court found that CSLI is even more invasive than the GPS data that was at issue in *Jones* because, unlike a vehicle that you exit when not traveling, most people always carry their phones with them providing comprehensive data more comparable to wearing an ankle monitor.[113] Additionally, carriers are collecting the data of all users—not just those suspected of crimes—for five years.[114] This gives police retrospective access to five years*'* worth of comprehensive location data and *"*[o]nly the few without cell phones could escape this tireless and absolute surveillance.*"*[115] Thus, the Court held that the Government violated Carpenter*'*s reasonable expectation of privacy in his physical movements when it obtained CSLI data from his wireless carriers.[116]

Next, the Court analyzed the Government's contention that the records were exempt from the Fourth Amendment protections by the third-party doctrine principles because Carpenter willingly conveyed his location to the wireless carriers.[117] However, the Court distinguished CSLI from the other business records implicated in *Smith* and *Miller* stating that, at the time of those cases, one could not have imagined a person carrying a cell phone with him everywhere logging his every move would become so commonplace.[118] It also reiterated that sharing information with a third party does not remove the expectation of privacy, but rather *"*diminishe[s

110. *Id.* at 2214-15.
111. *Id.* at 2215.
112. *Id.* at 2217.
113. *Id.* at 2218.
114. *Id.*
115. *Id.*
116. *Id.* at 2219.
117. *Id.* at 2219-20.
118. *Id.*

the] privacy interests.*"*[119] Finally, the Court addressed the voluntary nature of the conveyance of CSLI, noting that using a cell phone necessarily creates CSLI, which cannot be avoided, and thus, the user cannot *"'*assume[] the risk*'* of*"* conveying the entirety of his movements.[120] Consequently, the Court declined to extend the third-party doctrine to CSLI holding that, because of the *"*unique nature*"* of being constantly logged, a user can maintain a claim to Fourth Amendment protections in their own cell phone location records even if they are maintained by a third party.[121] Given that Carpenter had a reasonable expectation of privacy in the CSLI data and the Government accessed it, the Court concluded that a Fourth Amendment search had occurred.[122]

Lastly, the Court concluded that the Government must meet the standard of a warrant supported by probable cause when seeking CSLI data.[123] Carpenter's records were obtained by using the lower standard which is specified by the Stored Communications Act, but the Court held that is not a permissible method by which to gather CSLI.[124] Although Justice Alito in his dissent argued that implementing this standard is a significant departure from precedent,[125] the majority distinguished this case stating, "this Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy."[126] Even so, the Court reasoned "that CSLI is an entirely different species of business record," and the Court should be cautious to extend precedents to new digital technology indiscriminately.[127] It clarified later that a "warrant is [only] required in the rare case where the suspect has a legitimate privacy interest in [the] records held by a third party."[128]

119. *Id.* at 2219.
120. *Id.* at 2220 (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).
121. *Carpenter*, 138 S. Ct. at 2220.
122. *Id.*
123. *Id.* at 2221.
124. *Id*.
125. *Id.* at 2247 (Alito, J., dissenting).
126. *Id.* at 2221 (majority opinion).
127. *Id.* at 2222.
128. *Id.*

B. Carpenter *Dissent Suggests a Traditional Fourth Amendment Argument*

The *Katz* reasonable-expectation-of-privacy-test is not the only way to evaluate if a person has a Fourth Amendment right to privacy in his data. Another possible analysis is the age-old common-law property analysis. The 5-4 decision in *Carpenter* spurred four separate dissents, and it is the dissent authored by Justice Gorsuch that inspired the second analytical framework in this Note. Justice Gorsuch highlights the vulnerabilities of Fourth Amendment protections in a digital age where many people are resorting to online options to run the entirety of their lives, thus exposing personal papers and effects that were once kept private to third parties.[129] He then outlines three possible options for how to approach this issue, the third of which he admits many courts have grown rusty in applying—a traditional property-based Fourth Amendment analysis.[130]

Although this property-based approach is not new, it has not been consistently applied in this new world of data-producing, internet-connected devices; Justice Gorsuch has some ideas about how that will work.[131] To review, a traditional property-based Fourth Amendment analysis first examines whether the information in question belongs to a person by law.[132] Additionally, that property interest must be of the type that is protected by the Fourth Amendment; traditionally houses, persons, paper, and effects.[133] Next, if the information has been shared with a third party, the analysis determines if the original owner can retain an interest that is significant enough to warrant Fourth Amendment protections.[134] The last step is to determine under what standard the data could be compelled, either by a warrant supported by probable cause or some other means.[135]

All four dissents seem to prefer this original Fourth Amendment interpretation. Fortunately for Carpenter, it would be indisputable that the cell-site records were the type of data covered by the Fourth Amendment because they are his location data. The Court has already recognized that

129. *Id.* at 2262 (Gorsuch, J., dissenting).
130. *Id.* at 2262-72.
131. *Id.* at 2267-72.
132. *Id.* at 2267-68.
133. *Id.*
134. *Id.* at 2268.
135. *See id.*

a person has a right to be secure in his movements.[136] Unfortunately for Carpenter, and more broadly CSLI, only Justice Gorsuch even briefly considered that Carpenter might have had a common-law property interest in his own CSLI based on the Telecommunications Act.[137] But Justice Gorsuch notes that Carpenter did not develop the argument further by looking for any state law that might support the claim or preserve it for appeal.[138] However, the three other dissents dismissed the idea of a property interest in short order finding that "[h]e did not create the records, he does not maintain them, he cannot control them, and he cannot destroy them,"[139] that "[the Telecommunications Act] does not grant cell phone customers any meaningful interest in cell-site records,"[140] and finally that "Carpenter indisputably lacks any meaningful property-based connection to the cell-site records owned by his provider."[141] Based on those opinions, it is unlikely Carpenter would have prevailed in establishing a legitimate property interest in his CSLI data using a property-based analysis even though it is the type of data that the Fourth Amendment protects.

However, had he been able to establish a property interest in the CSLI, then Justice Gorsuch posits that his Fourth Amendment protections do not disappear simply because a third party has access to his papers or effects.[142] The purpose of the third-party doctrine is not to remove a person's security in his property, but rather to "place[] necessary limits on the ability of individuals to assert Fourth Amendment interests in property to which they lack a 'requisite connection.'"[143] Justice Gorsuch relies on the concept of bailment to establish this right to retain a property interest when a third party holds data, specifically mentioning *Ex parte Jackson*[144] where the Court held that letters in the mail were subject to the same Fourth Amendment protections as letters in a person's house.[145] Likewise, Justice Kennedy admits that "*Miller* and *Smith* may not apply when the Government obtains the modern-day equivalents of an individual's own

136. *Id.* at 2217 (majority opinion).
137. *Id.* at 2272 (Gorsuch, J., dissenting).
138. *Id.*
139. *Id.* at 2235 (Thomas, J., dissenting).
140. *Id.* at 2229 (Kennedy, J., dissenting).
141. *Id.* at 2260 (Alito, J., dissenting).
142. *Id.* at 2268 (Gorsuch, J., dissenting).
143. *Id.* at 2227 (Kennedy, J., dissenting) (quoting Minnesota v. Carter, 525 U.S. 83, 99 (1998) (Kennedy, J. concurring)).
144. *Ex parte* Jackson, 96 U.S. 727 (1877).
145. *Id.* at 733.

'papers' or 'effects,' even when those papers or effects are held by a third party."[146] The Sixth Circuit relied on this same concept when holding that Warshak retained a Fourth Amendment protection to emails stored on a third-party server.[147] This bailment property concept should be used as a part of the property-based analysis to evaluate when the third-party doctrine applies to unavoidable digital data.

Because the Fourth Amendment only protects against unreasonable searches and seizures, the final step in the traditional Fourth Amendment analysis is to examine what standard makes a search of digital data reasonable. Since this Note recommends the use of this analysis for data that is held by a third party, the third-party doctrine exception—that when information is shared with a third party, the government can compel the third party to produce the data without a warrant—is implicated. However, because the analysis relies on bailment concepts to establish that the requisite property interest is not extinguished by sharing the data with cell phone providers, *Ex parte Jackson* is the case that is most on point for this analysis. "No one thinks the government can evade *Jackson*'s prohibition on opening sealed letters without a warrant simply by issuing a subpoena to a postmaster."[148] Therefore, it is appropriate to ask if the type of data in question is close enough to letters in the mail that subpoenas would not be sufficient to obtain the data from a third party.

Riley v. California provides another perspective that might be helpful in this part of the analysis because the Court held that cell phone data could not be searched incident to an arrest without a warrant.[149] The third-party doctrine and the search incident to arrest are similar because they are both types of exceptions to the warrant requirement of the Fourth Amendment. It is reasonable to conclude that if cell phone data could not be searched without a warrant because of the search incident to an arrest exception, then it also could not be acquired from a third-party, such as a cloud service, pursuant to the third-party doctrine exception. Therefore, *Riley* could be used to reason that some types of digital data should not be acquired from a third party or otherwise without the use of a warrant supported by probable cause.[150]

146. *Carpenter*, 138 S. Ct. at 2230 (Kennedy, J., dissenting).
147. United States v. Warshak, 631 F.3d 266, 285-86 (6th Cir. 2010).
148. *Carpenter*, 138 S. ct. at 2271 (Gorsuch, J., dissenting).
149. Riley v. California, 134 S. Ct. 2473 (2014).
150. *Id*.

IV. FOURTH AMENDMENT APPLICATION TO SMART SPEAKER DATA

A. Applying Carpenter *to Smart Speaker Data*

Because the Court's decision in *Carpenter* hinged on the unique qualities of CSLI that distinguished it from other types of business records, a proper application of the holding in *Carpenter* to smart speaker data—or any other type of unavoidable digital data held by a third party—begins with an analysis of the data type in question and an inquiry of whether a person has a legitimate expectation of privacy in that type of data. The Court recommends two guideposts to assist in the analysis: "to secure the 'privacies of life' against 'arbitrary power'" and "to place obstacles in the way of a too permeating police surveillance."[151] After establishing that expectation, the analysis turns on whether the type of data is such that the privacy interest remains when the information is shared with a third party and thus survives the third-party doctrine. The final analysis looks at what standard is needed to properly request production of the data.

The Court in *Carpenter* easily connected the comprehensive location information collected by cell towers to the recognized right to privacy in the whole of one's movements.[152] Such a connection would not be proper when evaluating smart speaker data. While the data collected by a smart speaker could implicate the comings and goings of a person—for instance, if a user regularly interacts with the device to activate his home alarm and door locks—it does not necessarily create a comprehensive log of the user's movements like CSLI.

However, the stored smart speaker data are recordings of all the interactions that the user has had with all the voice-assistant connected devices in the user's home. These in-home interactions would necessarily be considered the type of "privacies of life" the Fourth Amendment seeks to secure. Additionally, the Court in *Berger* effectively brought conversations fully under the protection of the Fourth Amendment when stating that *Silverman* recognized that the Fourth Amendment protects the "overhearing of verbal statements" as well as the "seizure of 'papers and effects'" and ultimately held that police must obtain a warrant supported by probable cause to install a wiretap.[153] Just as the CSLI provides

151. *Carpenter*, 138 S. Ct. at 2214.

152. *Id.* at 2213-15.

153. Berger v. New York, 388 U.S. 41, 51-52 (1967) (quoting Wong Sun v. United States, 371 U.S. 471 (1963)).

comprehensive movement records far beyond the previous technology of GPS data, smart speaker data records are far more comprehensive than the conversations that were overheard in *Silverman* because the data can include not only voice recordings (conversations) but also information about many other aspects of a user's life: calendar appointments, internet searches, music selections, home entry and exit, shopping lists, and to-do lists to name a few. The Court addressed a similar issue in *Riley* concerning cell phones and held that these same data types being housed on a cell phone elevated the Fourth Amendment protections that a person has in that device.[154] Using this analogy of smart speaker data to that of conversations and cell phone data, it is reasonable to conclude that a person has a legitimate expectation of privacy in the type of data that is collected and stored by smart speakers.

Likewise, society has an expectation that law enforcement would not be able to monitor all the interactions happening inside a person's home for an extended time period.[155] Although smart speakers are not as common as cell phones, the adoption rate of speakers is rapidly growing.[156] Just as the Court reasoned that "[o]nly the few without cell phones could escape" constant surveillance,[157] even those without smart speakers can be exposed to surveillance when visiting friends and family members with the device in their homes. Furthermore, like CSLI, the smart speaker data is collected and retained over a long period of time for criminals and law-abiding citizens alike "giv[ing] police access to a category of information otherwise unknowable."[158] However, unlike CSLI, a user has access to smart speaker data and can delete recordings or interactions. Nevertheless, it seems unreasonable that the only way to protect oneself from retrospective police surveillance would be to delete your own data and make your voice assistant experience less effective. Therefore, the expectation of privacy in a user's smart speaker data is one that society readily recognizes, and allowing government officials access to potentially comprehensive smart speaker records implicating the goings-on inside the home would be contrary to that expectation.

Next, because the smart speaker data is collected and stored by a third party, it is necessary to examine the nature of the data in question to

154. *Riley*, 134 S. Ct. at 2493.
155. Kyllo v. United States, 533 U.S. 27, 33 (2001).
156. Marr, *supra* note 3.
157. *Carpenter*, 136 S. Ct. at 2218.
158. *Id.*

determine if there is a legitimate expectation of privacy in its contents that make it distinct from the business records in *Smith* and *Miller* to determine whether the third-party doctrine applies.[159] The analysis considers the limits of the data collected, the expansiveness of the data, and the voluntariness of allowing a third party to access the data.

Like the cell phone carriers use of CSLI for their own business purposes, voice assistant service providers use the data that is collected from smart speakers to improve their processes and to make their voice assistants smarter.[160] However, it is well-established that simply because a third party is allowed or requires access to your property, you do not immediately lose all Fourth Amendment protections.[161] And unlike the cell-site records at issue in *Carpenter*, which Carpenter did not create or possess or have rights to access, modify, or destroy, smart speaker data is created by the user when interacting with the device, stored by the service in the user's account, and accessed by the user to review and destroy if desired. Furthermore, the types of records included in the smart speaker data are much more expansive than the types explored in *Smith* and *Miller*. And just as there is no meaningful limit on the information provided by CSLI,[162] the data collected by smart speakers suffers from similar limitlessness.

Finally, the Court observed that a cell phone user cannot avoid sharing his location with wireless carriers unless he elects to turn off all his network services crippling the ability to use the cell phone fully. Similarly, a smart speaker user can delete content from her account to protect it from prying eyes, but that comes with a trade-off resulting in reduced accuracy of the device and limiting the device from operating to its fullest capacity. Therefore, the type of data collected by smart speakers is much more akin to the CSLI in *Carpenter* than the simple business records in *Smith* and *Miller*, and just as a person retains an expectation of privacy in his location records that are maintained by wireless carriers, users retain a legitimate expectation of privacy in the data that is retained by voice assistant services.

The final analysis in *Carpenter* determines the standard by which the government must comply to obtain data records from a third party. The holding is clear, "a warrant is required in the rare case where the suspect

159. *Id.*
160. Marr, *supra* note 3.
161. *Carpenter*, 138 S. Ct. at 2269-70 (Gorsuch, J., dissenting).
162. *Id.* at 2219 (majority opinion).

has a legitimate privacy interest in records held by a third party."[163] As previously discussed, under a *Carpenter*-style analysis, a user retains a legitimate privacy interest in the data that is maintained by voice assistant services. Thus, if the government wants to obtain those records, it would first need to get a warrant supported by probable cause, unless there are exigent circumstances. This is appropriate because smart speaker data—just like CSLI—"is an entirely different species of business record,"[164] and allowing the data to be subpoenaed under a less stringent standard would allow a user's Fourth Amendment rights to be circumvented.

1. Pros of Using a *Carpenter*-Inspired Analysis

The analytical framework modeled by the Court in *Carpenter* has some benefits when used as a model to evaluate how to assess the Fourth Amendment applicability to unavoidable digital data. First, it acknowledges that digital data is different. The Court in *Carpenter* repeatedly acknowledges that CSLI data is "unique" and categorically different than the records that precedent has considered.[165] This is a great first step to bringing the Fourth Amendment into the digital age. The analysis requires a deep understanding of the type of data that is in question and then looks to find an analogous pre-digital precedent. The result is a rich but subjective analysis that fully considers the implications of the data and then thoughtfully extends or declines to extend a precedent. Second, it errs on the side of protection of Fourth Amendment rights. Applying the standard of a warrant with probable cause to searches of data held by third parties is a significant extension of Fourth Amendment rights. Finally, it provides a framework where none previously existed. Prior to *Carpenter*, there was a lot of uncertainty about how to apply the Fourth Amendment in the digital age where much of what was previously held privately by people is now entrusted to third parties. While it does not answer all—or even many—of those questions, it does provide some guidance as to a structure that the courts can use when faced with Fourth Amendment digital data cases.

163. *Id.* at 2222.
164. *Id.*
165. *Id.* at 2217.

2. Cons of Using a *Carpenter*-Inspired Analysis

While some framework is better than no framework, the analysis used by the Court in *Carpenter* does present issues when attempting to apply it to other types of data. First, the Court specifically limits the application of the decision stating that it is not "express[ing] a view on matters not before us."[166] This could discourage lower courts from applying the framework or accepting the framework when applied to data other than CSLI. Second, the framework is complicated. Justice Gorsuch sums it up in his dissent:

> Lower courts should be sure to add two special principles to their *Katz* calculus: the need to avoid "arbitrary power" and the importance of "plac[ing] obstacles in the way of a too permeating police surveillance." While surely laudable, these principles don't offer lower courts much guidance. The Court does not tell us, for example, how far to carry either principle or how to weigh them against the legitimate needs of law enforcement.[167]

After the intense "*Katz* calculus,"[168] the lower courts must grapple with the multifactored third-party considerations.[169] With so many steps and little specific guidance in the analytical process, it is certain that courts will come to differing conclusions about similar data types. While some questions may be answered with the framework, it is sure to create many more questions, and circuit splits are likely, which will result in the need for additional guidance from the Court in how to apply the multi-faceted analysis.

Finally, the analysis creates significant uncertainty for law enforcement when attempting to use the compulsory process to obtain records. The seemingly arbitrary six-day limit of CSLI before a warrant is needed, coupled with the general requirement of obtaining a warrant with probable cause will make it difficult for investigations to comply with the correct compulsory process.[170] Under this ruling, whenever the government seeks data, it will first need to conduct the multifactor third-party data analysis to determine if the suspect maintains a legitimate

166. *Id.* at 2220.
167. *Id.* at 2266 (Gorsuch, J., dissenting) (quoting majority opinion at 2214).
168. *Id.*
169. *Id.* at 2234 (Kennedy, J., dissenting).
170. *Id.*

privacy interest in the data to know what compulsory process to use. Evidence obtained without the proper procedures is threatened by the exclusionary rule. The result could be a complication of the investigatory processes and an impediment to the government's ability to conduct timely and effective investigations.[171] Furthermore, the holding invalidates the standard created by legislatures to govern how CSLI can be gathered from third parties and could prevent positive law from developing by creating this expansion of the constitutional protections of the Fourth Amendment.[172]

B. Applying Traditional Fourth Amendment Doctrine to Smart Speaker Data

A proper application of the traditional common-law property-based approach to Fourth Amendment doctrine first examines the data type in question to determine if the person has the requisite common-law property interest in the data and if the data is of the kind that is protected by the Fourth Amendment. Next, if there is a property interest that is protected by the Fourth Amendment, one must analyze to what extent that interest remains when the data is shared with a third party. Finally, the standard or method by which the government can compel production of the data must be determined to ensure compliance with Fourth Amendment rights.

As each *Carpenter* dissent indicated, a person must look to positive law to establish a common-law property interest in digital data. Although *Carpenter* failed to establish that a person can have a property interest with respect to CSLI, smart speaker data is unlikely to suffer the same fate. Unlike CSLI, to which a user retains no control because it is generated by the cell phone towers and maintained and controlled by wireless carriers,[173] a smart speaker user can control nearly all aspects of the data collected by voice assistant services. The user creates the data when interacting with the speaker. The user determines the nature of the data by selecting what features to use and what devices to connect to the voice assistant. The voice assistant service saves the records of interactions in the users account and the user can log in to view the records and maintain or even destroy them. Given the immense control that the user maintains over the records, a user clearly has a significant property interest in the

171. *Id.*
172. *Id.*
173. *Id.* at 2235 (Thomas, J., dissenting).

data that is being stored on the voice services' system.

Even with a property interest established, a traditional analysis requires that the property type be within the scope of the text of the Fourth Amendment. Traditionally, that means the data must fall within one of the four identified categories: persons, houses, papers, and effects. While smart speaker data could not be considered persons or houses, it certainly could fall into the categories of papers and effects. We can look at recent precedent to observe how the Fourth Amendment is applied to similar digital data. *Riley* explored similar personal digital data that was stored on cell phones and found that Fourth Amendment protections do apply.[174] The Court in *Riley* recognized that a cell phone is not like other non-digital items a person might carry because of the multiplicity of functions and quantity of data that can be stored on a cell phone.[175]

Like the cell phone, smart speaker data can include the user's internet search history, purchase history, calendar items, and notes. Smart speaker data can also include detailed information about what happens in a user's home, such as when televisions and lights are turned off and on, when doors are opened and closed, and when the alarm is set. Additionally, all of the user's verbal commands and requests are stored on the servers until the user decides to delete them. These verbal commands are communications with the artificial intelligence machine that is behind the smart speaker. Finally, though voice assistant service providers insist that they only record commands and requests, it is entirely possible that the collected data could include conversations that take place in the home—which has, in fact, happened. This potential data set could be used by law enforcement to reconstruct "[t]he sum of an individual's private life" just as much as cell phone data.[176] Therefore, smart speaker data should be regarded as modern-day papers and effects that hold for those that use them in the "privacies of life" and would be the type of property covered under the Fourth Amendment.[177]

Next, since smart speaker data is necessarily shared with a third party, we must evaluate to what extent the user's property right is diminished by that act of sharing to ensure that the user maintains enough of a property interest to retain his Fourth Amendment protections in the data. While Amazon, Google, or Microsoft (as voice assistant service providers) have

174. Riley v. California, 134 S. Ct. 2473, 2484 (2014).
175. *Id.* at 2489.
176. *Id.*
177. *Id.* at 2495 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

a right to use the data they collect from their users, we know that right of access or use does not extinguish a property interest.[178] In his dissent to *Carpenter*, Justice Kennedy admitted that even when a person's modern-day papers and effects are held by a third party, the third-party doctrine might not apply when the Government obtains them.[179] Justice Gorsuch recommended the use of a bailment property concept to reconcile the third-party access and use issue with digital data.[180] "A bailment is the 'delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose.'"[181] This concept is not new to Fourth Amendment jurisprudence and is appropriate for inclusion in a traditional property-based analysis.[182]

In *Ex parte Jackson*, the Court found that the sender maintained a property interest in letters that were in the mail because "[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers . . . wherever they may be."[183] This concept of Fourth Amendment rights for persons who send letters in the mail should be applied to situations where a user must entrust her property data to a voice assistant service provider. A user should not forfeit her security in her data simply because she must allow the voice assistant service provider to access the data for the limited purpose of providing service to her.

Thus, applying the bailment concept to smart speaker data yields promising results. The user (or bailor) sends her data to the service provider (or bailee) by interacting with the smart speaker. The user chooses what data is on the server not only by choosing commands and requests, but also by determining the devices that are connected and controlled by the voice assistant software. It is through these conscious decisions that the user determines what data will be shared with the voice assistant service provider. Then by logging into her account and updating account settings, the bailor also indicates to what extent the bailee can use the data for its own business purposes. This process of data sharing shows that, even though the data is being held by a service provider, the user retains significant control over the data.

178. *Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting).
179. *Id.* at 2230 (Kennedy, J., dissenting).
180. *Id.* at 2268-70 (Gorsuch, J., dissenting).
181. *Id.* at 2268.
182. *Id.*
183. *Ex Parte* Jackson, 96 U.S. 727, 733 (1871).

The two cases that have surfaced to date show that Amazon seems to respect the user's preferences and control. For instance, in the *Bates* case that was referenced earlier in this Note, Amazon was compelled to turn over Bates' smart speaker data to the government, but Amazon initially refused to comply because it felt the warrant was overbroad, not specific enough, and possibly violative of the First Amendment.[184] However, when Bates gave them permission to release the data, they immediately did so.[185] The warrant did not change, but once Bates had given his permission for the data to be provided to law enforcement, Amazon respected his wishes; possibly because they believed that the data ultimately belonged to Bates, and he could permit the sharing. These facts support the proposition that the data is owned by the user and is simply being held in bailment by Amazon. Therefore, it is reasonable to conclude that the user retains a significant property interest in their own smart speaker data and would not lose Fourth Amendment protections by allowing a voice assistant service provider to access and use the data.

Finally, we can use the traditional Fourth Amendment analysis to determine under what standard the government can obtain the smart speaker data while still adhering to the reasonable search and seizure requirement of the Fourth Amendment. In *Ex parte Jackson*, the Court established that letters in the mail have the same Fourth Amendment protections as papers in the home and that the government must obtain a warrant based on probable cause before seizure and inspection of letters that are in the mail.[186] The Sixth Circuit declared email to be the "technological scion" of letters in the mail and reached the same conclusion concerning the need for police to obtain a warrant supported by probable cause before compelling an internet service provider to hand over email communications.[187]

Just like the letters that are in bailment with the postal service and the email that is in bailment with the internet service provider, smart speaker data that is in bailment with a voice assistant service provider should retain the same level of protection as that data would be afforded if it were found in the home. While not all of the smart speaker data is communicative in nature, it is similar in nature to the digital cell phone data that was explored in *Riley*. And, in *Riley*, the Court found that neither the police need for

184. McLaughlin, *supra* note 6.
185. *Id.*
186. *Ex parte* Jackson, 96 U.S. at 733.
187. United States v. Warshak, 631 F.3d. 266, 286 (2010).

protection nor preservation of evidence was a compelling enough reason to bypass the warrant requirement, generally, before accessing a suspect's cell phone data.[188] Therefore, since smart speaker data is sufficiently similar to the data on a cell phone and is being held in bailment by a third party (like letters and emails), then these three cases taken together support that a warrant based on probable cause would generally be required before police could access smart speaker data.

1. Pros of Using Traditional Fourth Amendment Analysis

A traditional property-based analysis for smart speaker data provides notable benefits over using the *Carpenter* exception to the third-party doctrine. First, it provides a less complicated, more objective framework for analysis. As mentioned previously, the Court adds two layers to the *Katz* test in *Carpenter* and creates a model for an intricate, multifaceted third-party doctrine analysis.[189] Both of which will require a subjective application of lower courts' discretion because neither is well defined by the Court or otherwise. By contrast, a traditional analysis uses analogies to positive law which are less subjective in nature. Additionally, the traditional Fourth Amendment approach does not need to apply a multifaceted third-party analysis because it simply relies on property principles, like bailment, which are already well-defined. Establishing a property interest immediately implicates Fourth Amendment protections against unreasonable search and seizure.[190] Reliance on established principles of law makes application of this method much simpler for the courts.

Second, because it relies on positive law, this method allows for and encourages the development of positive law. This is incredibly important as it relates to digital data because it is impossible for the Supreme Court to keep up with the speed that technology is advancing.[191] States are already realizing this and beginning to enact laws to protect their citizens' privacy.[192] By relying on positive law to guide the justice system rather

188. Riley v. California, 134 S. Ct. 2473, 2493 (2014).
189. *Supra* Part II.A.
190. Carpenter v. United States, 138 S. Ct. 2206, 2268 (2018) (Gorsuch, J., dissenting).
191. *Id.* at 2206, 2233 (Kennedy, J., dissenting).
192. *Id.* at 2270 (Gorsuch, J., dissenting). *See also* Jason Tashea, *California Imposes New Regulations on 'Internet of Things' Devices*, ABA JOURNAL (Dec. 10, 2018, 7:00 AM),
http://www.abajournal.com/news/article/new_california_imposes_regulations_on_the_int

than relying on the judge to determine what society is prepared to recognize as reasonable, the lawmaking power is returned to the elected representatives of the people where it belongs.

Third, property-based arguments are closer to the true language of the Fourth Amendment. "The Fourth Amendment guarantees individuals the right to be secure from unreasonable searches [and seizures] of 'their [own] persons, houses, papers, and effects.'"[193] Thus, by requiring the person to establish a property right to the data in question, it is much closer to the textual intent of the Constitution, which implies that you cannot have a Fourth Amendment interest in someone else's property.

Finally, the *Katz* doctrine relied on in *Carpenter* is coming under more scrutiny. In *Carpenter*, four of nine justices call for it to be overturned with one referring to the *Katz* test as a "failed experiment."[194] One concern with the reasonable-expectation-of-privacy test is that it can both shrink and enlarge the protections that are covered under the Fourth Amendment and is not true to the text of the Constitution.[195] Because the traditional common-law property analysis does not rely on the *Katz* test, which is at the mercy of the Court, but rather relies on constitutional language and well-established principles of property, it provides an element of predictability and consistency for the protection of digital data.

2. Cons of Using Traditional Fourth Amendment Analysis

But the traditional common-law property analysis is not without its own complications. Much of the data collected by smart speakers are recordings of *conversations* with the user and the artificial intelligence machine that is behind the voice services, and the remainder of the data is information about other interactions that the user has with the speaker and any devices that are connected. While I analogized that data to cell phone data in this Note to apply the property framework, there is still uncertainty about how to establish a property interest and what positive law would be applied.[196] For instance, although I made arguments here for the bailment theory, it is unclear what common-law rule applies when a party is subpoenaed to produce someone else's documents with which he has been

ernet_of_things/ [https://perma.cc/96L9-9AN8].

193. *Carpenter*, 138 S. Ct. at 2206, 2235 (Thomas, J., dissenting).
194. *Id.* at 2246 (Thomas, J., dissenting).
195. *Id.*
196. *Id.* at 2268 (Gorsuch, J., dissenting).

entrusted.[197] Additionally, while the framework leaves room for legislative and common-law provisions, those are not in place yet. The courts and legislatures are faced with developing that law to ensure digital data is afforded the appropriate protections under the Fourth Amendment. But until the positive law catches up with technology, there is still a risk that some protections will not be secured in the meantime. Finally, the limitations of a property-based analysis may be what caused the birth of *Katz*; therefore, to return to a more limited view of what is covered might encourage more judicial activism in efforts to secure the rights of the people.

C. Propose the Analytical Framework to Apply

Although the Court chose to apply the *Katz* reasonable-expectation-of-privacy test in the *Carpenter* case, it is not necessarily the model that should be followed for all digital data applications. While it is tempting to simply use the framework in *Carpenter* to analyze smart speaker data, it is also important to remember that the *Katz* test did not displace the property-based analysis, but rather just added to it. The majority likely realized that, had the Court applied a traditional property-based analysis in *Carpenter*, the result would not have been favorable for Carpenter because he seemed to lack the requisite property interest in the data to which he was claiming Fourth Amendment rights. Therefore, it was necessary to use the *Katz* test and find an exception to the third-party doctrine to ensure his data was protected by the Fourth Amendment.

However, in the case of smart speaker data—as well as similar types of digital data held by third parties—it is much easier to establish property rights and, thus, potential Fourth Amendment protections. It is not necessary to over-complicate the analysis with additional *Katz* considerations and subjective third-party doctrine applications at every turn. The traditional property-based Fourth Amendment analysis should be used for smart speaker data because it provides a practical framework that allows for positive law to drive the protection of data privacy rights. Additionally, it is truer to the text of the Constitution because it requires that a person have a legitimate property interest in the information to which they are claiming Fourth Amendment rights. This property requirement keeps the Fourth Amendment from being turned into a general right to privacy while still allowing for the protection of personal

197. *Id.*

digital data (a.k.a. property) that is necessarily shared with or stored by a third party just like physical property. The test also requires that the property be of the type that is covered by the Fourth Amendment, i.e., persons, houses, papers, and effects, which once again prevents from over broadening the provision, but still extends the protections to modern day analogues. If data privacy laws develop in lockstep with technological advances, using the property-based Fourth Amendment application is all that is needed to "assure[] preservation of that degree of privacy against government . . . when the Fourth Amendment was adopted."[198]

Based on the precedent discussed in this Note,[199] the establishment of a legitimate property interest in data held by a third party naturally leads to requiring law enforcement to obtain a warrant supported by probable cause before compelling the third party to turn over data. While this proposal would no doubt be troubling to all the dissenting justices except Justice Gorsuch, their analysis was based on the presumption that Carpenter did not have any legitimate property interest in the CSLI data. Smart speaker data, absent a property interest by the user, would be termed business records, and compelling records from businesses should traditionally be subjected to the *Oklahoma Press* standard discussed in Alito's dissent.[200] However, there is no direct precedent for what standard should be used when the third party is holding the data in a bailment for the user.[201] Should this be a higher standard than *Oklahoma Press*? I think so, and I posit that a warrant supported by probable cause would be the most supported by current analogous precedents. There is room for positive law to make this decision, and there is no need for the Court to make this decision as it did in *Carpenter*. Though some justices expressed concern that this requirement will have a negative effect on the police's ability to conduct investigations,[202] the standard will only apply when the user maintains a property interest in the information that is sought. While this will create some uncertainty initially for police investigations, hopefully it will push lawmakers to fill the gap in positive law to address the uncertainties.

198. *Id.* at 2214 (citing Kyllo v. United States, 533 U.S. 27, 34 (2001)).
199. *See supra* Part II.B.
200. *Carpenter*, 138 S. Ct. at 2255-56 (Alito, J., dissenting). *See* Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186 (1946).
201. *Id.* at 2271 (Gorsuch, J., dissenting).
202. *Id.* at 2256-57 (Alito, J., dissenting).

V. CONCLUSION

The biggest danger to Fourth Amendment rights is the failure of individuals to recognize that the traditional common-law property approach still lurks in the shadows waiting for people to remember that the *Katz* reasonable-expectation-of-privacy test added to, rather than displaced, their rights. Justice Gorsuch opines that "[n]eglecting more traditional approaches may mean failing to vindicate the full protections of the Fourth Amendment."[203] Carpenter failed to adequately develop the property argument and preserve it for appeal in his case, and he was not the only one to forfeit a property-based argument that same session.[204] Smart speaker users need not resort to the convoluted test used in *Carpenter* to secure their rights. They can simply use the common-law property principles to overcome the privacy risks that are forced upon them by the nature of engaging with our technologically connected world.

203. *Id.* at 2272 (Gorsuch, J., dissenting).
204. *Id.*