SMART HOME DATA PRIVACY AND AN EVOLVING FOURTH AMENDMENT

Dr. Laurie Thomas Lee*

When Timothy Verrill was accused of first-degree murder of two women at a home in New Hampshire, prosecutors believed that recordings of the attack were captured on the man's Amazon Echo smart speaker.[1] Amazon refused to release the customer information without a warrant,[2] but a judge ruled that the New Hampshire authorities could indeed examine the recordings that reside on Amazon's server.[3]

This case, among others, raises serious questions about privacy in a new era of smart homes, where smart in-home devices collect a wealth of data about a home's occupants and now provide a fruitful investigative tool for law enforcement. Smart home devices, such as smart TVs, refrigerators, robotic vacuums, security systems, thermostats, video doorbells, health sensors, lighting systems, automated window blinds, and more, are quickly becoming an integral part of the modern, internet-connected home.[4] Yet these smart technologies generate an unprecedented amount of personal data from within the homes, producing highly detailed and intimate accounts of peoples' lives that are often captured and stored by their service providers.[5] Some voice-activated devices, such as the Amazon Echo and Google Home, may even record background conversations while activated, unbeknownst to their owners.[6]

The exposure of these communications and data to law enforcement and others has been characterized as the "tip of the

 Professor, University of Nebraska-Lincoln, College of Journalism and Mass Communications. Ph.D. in Mass Media from Michigan State University. Dr. Lee teaches courses in media law and ethics and is a co-author of Communications Law: Practical Applications in the Digital Age, 3rd ed.

1. Kathleen McKiernan, *Alexa Served: Privacy Concerns Echoed in New Hampshire Case*, BOS. HERALD (Nov. 11, 2018, 12:00 AM), https://www.bostonherald.com/2018/11/11/alexa-served-privacy-concerns-echoed-in-new-hampshire-case/.

2. *Id.*

3. *Id.*

4. Rachel Segal, *Are Smart Homes a Smart Idea?*, PERSP., https://www.theperspective.com/debates/businessandtechnology/smart-homes-smart-idea/ (last updated 2020).

5. *Id.*

6. McKiernan, *supra* note 1.

iceberg"[7] for major privacy concerns. To what extent are conversations and other data carried by smart home devices and stored by their service providers lawfully available to law enforcement? What privacy protections exist for people in today's smart home?

While no judicial decisions or federal or state laws explicitly address the privacy concerns associated with smart home technologies, protection against government intrusions would seemingly come from the U.S. Constitution, where the Fourth Amendment protects against government searches and seizures in the home.[8] But while Fourth Amendment jurisprudence has been evolving, it has not kept pace with rapid advances in technology. Here, the Fourth Amendment would require that smart home users have an expectation of privacy in their personal data and communications and that society would consider that expectation of privacy to be reasonable.[9] How these two prongs of a test created in 1967 might apply to today's smart home technologies is unclear.

More importantly, smart home users face a well-established exception to Fourth Amendment protection known as the third-party doctrine.[10] Few citizens realize that when their personal information is voluntarily shared with a third party such as their internet or phone provider, those records may be accessed by the government.[11] Further review of this long-standing doctrine is warranted in a modern era of digital communications where smart technologies become a requisite part of life and meaningful consent is questioned.

How the courts treat the privacy of smart home technologies may ultimately depend on application of the landmark 2018 decision of *Carpenter v. United States*, where the Supreme Court held that the Fourth Amendment protects cell-site location information (CSLI).[12] In that case, the Court found that a person has a reasonable expectation of privacy in their CSLI, and the Court limited the application of the third-party doctrine. But the ruling was narrow; the Court called it a "rare case," leaving future courts to determine whether a person's interest in other personal records held by a third party will be protected.[13]

---

7. *Id.*

8. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.").

9. *See* Katz v. United States, 389 U.S. 347, 352 (1967) (holding that wiretapping violates an individual's reasonable expectation of privacy).

10. McKiernan, *supra* note 1.

11. *Id.*

12. 138 S. Ct. 2206 (2018). CSLI is a time-stamped record generated each time a phone connects to a cell site. *Id.* at 2211.

13. *Id.* at 2222.

This Article examines this evolving Fourth Amendment jurisprudence and the framework for assessing new technologies akin to those of the smart home. It considers the intrusiveness of government infringements and the applicability of the expectation of privacy standard to today's smart technologies. In particular, it evaluates and critiques the applicability of the third-party doctrine to smart home data, calling for further reconsideration of the doctrine. Smart home data should be given Fourth Amendment protection, requiring law enforcement to at least obtain a warrant instead of a lesser standard court order as permitted under the Stored Wire and Electronic Communications Act.[14] As consumer demand continues to grow for smart home devices, so too will the need for legal guidance and assurances that user privacy will be protected. Fourth Amendment jurisprudence will need to further evolve to address the advances in smart technologies and the new privacy challenges presented.

I. THE SCOPE OF SMART HOME TECHNOLOGY PRIVACY CONCERNS

The smart home is among the fastest-growing category of new technology.[15] Nearly one-sixth of households in the United States are currently outfitted with smart home technology.[16] More than half of renovating homeowners incorporate at least one smart device in their newly remodeled homes.[17] Indeed, by 2022, one research firm predicts sixty-three million homes will qualify as "smart."[18] This advance in home automation and assistance is expected to increase in popularity over the next decade.[19] By just 2025, the market is expected to grow to over $150 billion with a household penetration of more than fifty-nine percent.[20]

The widespread adoption of smart homes can be traced to the 2014 launch of Apple's iHome app, which enabled smart phones to control smart home devices.[21] Next came Amazon's digital assistance technology, namely Alexa, paired with its Bluetooth enabled Echo smart

14. 18 U.S.C. §§ 2701–13.

15. Rob Marvin, *Privacy Tops List of Consumer Smart Home Concerns*, PC (Mar. 4, 2019), https://www.pcmag.com/news/privacy-tops-list-of-consumer-smart-home-concerns.

16. Joseph Flynt, *Smart Homes Statistics—Fascinating Industry Trends*, 3DINSIDER (Feb. 11, 2020), https://3dinsider.com/smart-home-statistics/.

17. Megan Ray Nichols, *Home Automation Will Increase in Popularity in the Next Decade*, IOTEVOLUTION (June 25, 2019), https://www.iotevolutionworld.com/smart-home/articles/442528-home-automation-will-increase-popularity-the-next-decade.htm.

18. Patrick Lucas Austin, *What Will Smart Homes Look Like 10 Years from Now*, TIME (July 25, 2019, 6:18 AM), https://time.com/5634791/smart-homes-future/.

19. Nichols, *supra* note 17.

20. Flynt, *supra* note 16.

21. *Id.*

speaker.[22] Soon after, a multitude of smart home devices appeared offering consumers the benefits of cost and time savings, entertainment, and even companionship.[23] Security is offered by networked security cameras, pet and baby monitors, doorbell cameras, and Wi-Fi enabled garage door openers. Energy-savings are reaped through the use of smart thermostats, smart lights, and even smart toilets.[24] Home healthcare is advanced with remote patient monitoring, activity motion sensors, smart pillboxes, and wearables that track heart rate, galvanic skin response, and more.[25] Consumers also find convenience in a variety of smart appliances, such as ovens and refrigerators, that can regulate temperature and alert users that cooking is complete, a filter needs replacing, or a door has been left open. And yet the most popular types of smart home devices are those made for entertainment purposes, such as smart TVs which account for forty-three percent of smart device purchases.[26] As smart home technologies become more commonplace, consumers will come to rely on them more just as they do their smart phones. Indeed, the majority of Americans expect smart homes will be just as common as smart phones by the end of the decade.[27]

These smart home devices comprise what is known as the "Internet of Things," or IoT, which has increasingly become a privacy concern among privacy advocates and scholars.[28] The IoT not only amplifies prior privacy challenges, but creates new issues.[29] Such embedded and interconnected computing devices are stoking privacy concerns as they operate in the background, gathering, storing, transmitting, and sharing significant volumes of data about their users' homes, activities, and behaviors.[30] Indeed, the growth of smart devices means a significant

22. *Id.*
23. *Id.*
24. Nichols, *supra* note 17.
25. *Id.*
26. Flynt, *supra* note 16.
27. *Id.*
28. *See, e.g.*, Marie-Helen Maras, *Internet of Things: Security and Privacy Implications*, 5 INT'L. DATA PRIVACY L. 99 (2015); Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85 (2014); Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 1 (2014); Alexander H. Tran, *The Internet of Things and Potential Remedies in Privacy Tort Law*, 50 COLUM. J.L. & SOC. PROBS. 263 (2017); Corynne McSherry, *Who Will Own the Internet of Things? (Hint: Not the Users)*, EFF (Jan. 20, 2015), https://www.eff.org/deeplinks/2015/01/who-will-own-internet-things-hint-not-users; Gilad Rosner & Erin Kenneally, *Privacy and the Internet of Things: Emerging Frameworks for Policy and Design*, CTR. FOR LONG-TERM CYBERSECURITY, https://cltc.berkeley.edu/wp-content/uploads/2018/06/CLTC_Privacy_of_the_IoT-1.pdf (last visited July 26, 2021).
29. Rosner & Kenneally, *supra* note 28, at 2.
30. *Id.*

increase in the breadth of data collection, where the monitoring and data produced is fueled by an increasing number of available sensors that include microphones and cameras, some of which are always turned on.[31] This system of "sensorveillance" means an ever-increasing ability to "track individuals through the data trails they leave behind."[32] Then with the help of artificial intelligence and algorithmic and statistical modeling techniques, the melding of personal profile information results in extensive database compilations that paint a remarkably complete picture about an individual.[33] Solove has described this condition of "dataveillance" as "a method of watching . . . by collecting facts and data."[34] Kerr refers to the resulting phenomenon as the "mosaic theory," where much more is revealed by a combination of information than from any isolated record.[35] The issue of scale is further magnified by an IoT system of widespread distribution, where personal data is shared via Wi-Fi with other smart devices and ultimately through the internet to service providers and potentially others.

Not only is the breadth of data collection, retention, and sharing a privacy issue, so too is its depth.[36] Smart devices are designed to monitor people's activities, environments, physical bodies, and emotions; and such personal data can be especially intimate. In a white paper on *Privacy and the Internet of Things*, Rosner and Kenneally characterize some of the IoT risks to privacy as a collapse of private spaces, a loss of emotional privacy, and a loss of choice and meaningful consent.[37] For example, wearables track bodily functions, diminishing the sanctity of personal space, and various biometric sensors detect the look and sounds of people's emotional states.[38] All the while, consumers are not fully aware of what they are agreeing to and are unable to easily withdraw consent or change privacy settings.[39] Scholars recognize this

31. *Id.* at 7.

32. Andrew Guthrie Ferguson, *The Smart Fourth Amendment*, 102 CORNELL L. REV. 547, 551 (2017).

33. Rosner & Kenneally, *supra* note 28, at 7; *see, e.g.*, *Big Data Is Too Big Without AI*, MARYVILLE UNIV., https://online.maryville.edu/blog/big-data-is-too-big-without-ai/ (last visited July 12, 2021) (demonstrating how artificial intelligence algorithms are in high demand because they create extremely accurate consumer profiles by collecting data from social media, cell phones, etc.).

34. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 33 (Jack Balkin & Beth Noveck eds., 2004).

35. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012). As applied to Fourth Amendment doctrine, Kerr says mosaic theory asks, "whether a series of acts that are not searches in isolation amount to a search when considered as a group." *Id.* at 320.

36. *See, e.g.*, Gabriel Bronshteyn, *Searching the Smart Home*, 72 STAN. L. REV. 455, 485–86 (2020).

37. Rosner & Kenneally, *supra* note 28, at 9–11.

38. *Id.*

39. *Id.* at 10.

control over personal information as informational privacy.[40] Not only is privacy a right to be left alone, but it also encompasses intimacy, the limited access to oneself, and control over personal information.[41]

Smart home devices are also a part of concerning changes to what Nissenbaum refers to as the "norms of information flow," which can lead to privacy harms.[42] Informational norms consist of norms of appropriateness and norms of flow or distribution, and they occur in a context of place, politics, convention, and cultural expectation, governed by roles, expectations, actions, and practices.[43] Breaches of these norms, such as exposing personal information and restricting people's control, constitute a violation of "contextual integrity" and "are held to be violations of privacy."[44] Yet norms are constantly evolving[45] and may shift in the face of shrinking expectations, where every encroachment of privacy gradually diminishes society's expectations of privacy.[46] In an era of "sensorveillance," people should certainly expect smart home devices to be monitoring them most of the time.[47]

Because individuals also effectively permit their data to be shared with third-party service providers by virtue of activating and using their smart home devices, smart home technology tests the rules and responsibilities associated with voluntary disclosure. Petronio's communication privacy management ("CPM") theory offers a framework for how people self-disclose online and advances a rule-based system for explaining how individuals balance the risks and gains of disclosure and privacy.[48] CPM theory explains that people will self-disclose despite risk warnings as they tend to maximize rewards and minimize costs.[49] Yet, a person's ability to protect the boundaries around their private information online will greatly depend on the extent to which they understand how and by whom their information may be

40. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1125 (2002).
41. *Id.* at 1122–23.
42. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 137 (2004).
43. *Id.*
44. *Id.* at 145.
45. *See* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 83 (2013).
46. Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 873 (2002).
47. Justin Jouvenal, *Commit a Crime? Your Fitbit, Keyfob or Pacemaker Could Snitch on You*, WASH. POST (Oct. 9, 2017), https://www.washingtonpost.com/local/public-safety/commit-a-crime-your-fitbit-key-fob-or-pacemaker-could-snitch-on-you/2017/10/09/f35a4f30-8f50-11e7-8df5-c2e5cf46c1e2_story.html (citing Ferguson, *supra* note 32).
48. *See* Stephen Cory Robinson, *Self-disclosure and Managing Privacy: Implications for Interpersonal and Online Communication for Consumers and Marketers*, 16 J. INTERNET COM. 385, 386 (2017).
49. *Id.* at 393.

shared or used and the associated risks.[50] Even so, individuals may share responsibility for what happens to their shared information. While the theory asserts that individuals believe they have a right to own their personal information, one CPM "interaction maxim" posits that when personal information is shared, the recipient becomes a co-owner, around which different boundaries exist for sharing information.[51] In this case, both parties become responsible for co-managing the information, and both parties also share in the ethical responsibility to minimize harm to the discloser.[52] How the courts interpret the responsibility of smart home users and the voluntary nature of their data disclosures will affect how the third-party doctrine is applied.

Smart home devices and their data are not only coveted by advertisers, marketers,[53] and hackers;[54] they are also of value to law enforcement officers. For this reason, these devices are of special concern due to the Constitutional rights they implicate. Access to smart home devices means law enforcement can efficiently track and investigate suspects and criminal cases by following the data trails and digital fingerprints left behind. Law enforcement can make inferences from sensors that prove geographic, temporal, and other connections to a crime.[55] For example, geolocation may tie a suspect to a crime scene while health data can show heart rate and blood pressure changes during the commission of a crime. Electricity and water usage data taken from smart meters can alert law enforcement to a wide range of illicit behaviors.[56]

The government is increasingly relying on smart home technology as an investigative tool.[57] In late 2015, a case involved data taken from a victim's step-counting Fitbit.[58] Connie Dabate's Fitbit showed her

50. *Id.* at 394.

51. *Id.* at 391; *see* Sandra Petronio & Wesley T. Durham, *Communication Privacy Management Theory*, *in* ENGAGING THEORIES IN INTERPERSONAL COMMUNICATION: MULTIPLE PERSPECTIVES 309, 314 (Leslie Baxter & Dawn Braithwaite, eds., 2008).

52. Robinson, *supra* note 48, at 391.

53. *See* Stephanie Miles, *How 5 Brands Are Marketing with Smart Home Technology*, STREET FIGHT MAG. (Dec. 9, 2019), https://streetfightmag.com/2019/12/09/how-5-brands-are-marketing-with-smart-home-technology/#.XuZ9kp5Kg1A; Thierer, *supra* note 28, at 54; Rosner & Kenneally, *supra* note 28, at 10.

54. Tom Kellermann, *If Your Home Is Getting Smarter, Don't Leave It Vulnerable to Hackers: Cyber Strategist*, CNBC (Nov. 30, 2019), https://www.cnbc.com/2019/11/30/how-to-defend-your-smart-home-from-hackers-after-black-friday-buys.html.

55. Ferguson, *supra* note 32, at 560–61.

56. Sarah Murphy, *Watt Now?: Smart Meter Data Post-Carpenter*, 61 B.C.L. REV. 785, 787–88 (2020); Daniel Zwerdling, *Your Home Is Your . . . Snitch?*, MARSHALL PROJECT (May 24, 2018, 12:30 PM), https://www.themarshallproject.org/2018/05/24/your-home-is-your-snitch.

57. Bronshteyn, *supra* note 36, at 467.

58. Jouvenal, *supra* note 47.

moving around her Connecticut home long after her husband Richard Dabate claimed she had been murdered by intruders.[59] Investigators also gathered evidence from the home's smart alarm systems and a key fob to ultimately charge the husband with her murder.[60]

In June 2016, the U.S. District Court for the Southern District of California issued the first published warrant for smart TV data, seeking to obtain the viewing activity data from a Samsung Smart TV owned by a man who was previously convicted for possession of child pornography.[61] A year later came the first known case in the U.S. in which Google Nest surveillance camera footage and customer data were turned over in a warrant to federal authorities to investigate a fraud perpetrated by a rap crew in North Carolina.[62] From 2015 to 2018, governments have demanded data from Google's smart home division, Nest Labs, on at least 300 occasions, requesting information on as many as 525 accounts.[63] Yet in 2019, no smart home device "worried privacy advocates more than Amazon's surveillance doorbell, Ring," which had initiated over 600 partnerships with police departments to provide officers access to video footage of users within a specific geographic radius.[64]

Still, searches of smart speakers, such as Amazon's Alexa, have perhaps received the most public attention.[65] In a highly publicized conflict between Amazon and the Benton County, Arkansas prosecutor's office, police sought a warrant for records from an Amazon Echo after James Bates called police to report that his friend, Victor Collins, was found dead in his hot tub.[66] Bates, Collins, and another friend had gathered at Bates's home to watch television. After, the men decided to

59. *Id.*

60. *Id.*

61. Thomas Brewster, *That Time Cops Searched a Samsung Smart TV for Evidence of Child Abuse*, FORBES (Feb. 7, 2017, 2:20 PM), https://www.forbes.com/sites/thomasbrewster/2017/02/07/samsung-smart-tv-fed-search-child-pornography/#6f81bff617d7.

62. Thomas Brewster, *How an Amateur Rap Crew Stole Surveillance Tech That Tracks Almost Every American*, FORBES (Oct. 12, 2018, 9:56 AM), https://www.forbes.com/sites/thomasbrewster/2018/10/12/how-an-amateur-rap-crew-stole-surveillance-tech-that-tracks-almost-every-american/#13f6b47250f1.

63. Thomas Brewster, *Smart Home Surveillance: Governments Tell Google's Nest to Hand Over Data 300 Times*, FORBES (Oct. 13, 2018, 8:31 AM), https://www.forbes.com/sites/thomasbrewster/2018/10/13/smart-home-surveillance-governments-tell-googles-nest-to-hand-over-data-300-times/#66d068902cfa.

64. Matthew Guariglia, *Smart Home Tech, Police, and Your Privacy: Year in Review 2019*, ELEC. FRONTIER FOUND. (Dec. 21, 2019), https://www.eff.org/deeplinks/2019/12/2019-end-year-review-smart-home-tech-police-and-your-privacy.

65. Bronshteyn, *supra* note 36, at 464–65.

66. Tracy Neal, *Arkansas Judge Drops Murder Charge in Amazon Echo Case: Man Found Dead in Hot Tub in 2015*, ARK. DEM. GAZETTE (Nov. 29, 2017, 12:13 PM), https://www.arkansasonline.com/news/2017/nov/29/arkansas-judge-drops-murder-charge-amazon-echo-cas/.

get into Bates' hot tub, and then Bates went to bed.[67] In the morning, Bates discovered Collins in the hot tub.[68] During the investigation, police noticed an Echo in Bates's kitchen and proceeded to seek its contents. They believed the Echo may have been activated around the time of Collins' death because someone present that night recalled hearing music streaming through the device.[69] The Bentonville police served Amazon with a warrant, requesting recordings transmitted from the Echo to its servers.[70] Twice they objected, but eventually the company voluntarily turned over the information when defendant Bates consented. [71] Prosecutors ultimately found no evidence from the Echo device, and the judge dismissed the murder charge.[72] Nonetheless, this case sparked national concern for the possibilities and implications of a new avenue of investigation using smart speakers.[73]

These are just a few of the known cases where law enforcement agents have turned to smart home technology for investigative purposes. Most cases are not reported publicly.[74] It is nonetheless clear that leveraging data generated by smart home devices is quickly becoming an important tool for government agencies. Reliance on smart home data "will only continue to grow in sophistication and scope as more devices become connected" and provide even more resources for surveillance and investigation.[75] Balancing the interests of police power, technological advances, and citizens' privacy rights under the Fourth Amendment must then fall to the courts, in what Kerr refers to as a phenomenon of "equilibrium-adjustment."[76] Kerr contends that the Supreme Court adjusts Fourth Amendment protections over time in order to effectively restore the equilibrium of interests, resulting in

67. Eliott C. McLaughlin, *Suspect OKs Amazon to Hand Over Echo Recordings in Murder Case*, CNN BUS., https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html (last updated Apr. 26, 2017, 2:52 PM).

68. *Id.*

69. *Id.*

70. David Kravets, *Amazon Refusing to Hand Over Data on Whether Alexa Overheard a Murder*, ARS TECHNICA (Feb. 23, 2017, 12:58 PM), https://arstechnica.com/tech-policy/2017/02/amazon-wont-disclose-if-alexa-witnessed-a-murder/.

71. Eliott C. McLaughlin & Keith Allen, *Alexa, Can You Help With This Murder Case?*, CNN BUS, https://www.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/index.html (last updated Dec. 28, 2016, 8:48 PM); Neal, *supra* note 66.

72. *Id.*

73. Max Brantley, *Benton County Prosecutors Drop Amazon Echo Murder Case*, ARK. TIMES (Nov. 29, 2017, 12:31 PM), https://www.arktimes.com/ArkansasBlog/archives/2017/11/29/benton-county-prosecutors-drop-amazon-echo-murder-case.

74. Bronshteyn, *supra* note 36, at 468–69.

75. Ferguson, *supra* note 32, at 549.

76. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011); *see also* Bronshteyn, *supra* note 36, at 472.

hundreds of "equilibrium-adjustments" over the years.[77] Indeed, further adjustments are likely necessary to address the privacy protections of those living in the smart home.

II. THE LEGAL LANDSCAPE

No laws explicitly address the privacy of smart home technologies, yet government access to such data and communications implicate constitutional rights—particularly when done without a warrant.[78] However, Fourth Amendment jurisprudence pertaining to related technologies, such as cellphones, is evolving.[79] The applicable precedents of an expectation of privacy and third-party doctrine, as well as property rights and the sanctity of the home, are being questioned by the courts in the face of rapid technological change.[80] An understanding of the Fourth Amendment's evolving doctrine and the landmark case of *Carpenter v. United States* will shed light on how it may be applied to smart home technology and how further reconsideration of the law, particularly the third-party doctrine, is needed to further protect against such advances in technology.[81]

A. Fourth Amendment Jurisprudence

The Fourth Amendment protects the right of people "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,"[82] although its interpretation by the Supreme Court has varied, resulting in conflicting interpretations, exceptions, and a "patchwork of protections."[83] When first adopted, the Framers saw it as a means "to safeguard the privacy and security of individuals against arbitrary invasions by government officials"[84] after enduring a colonial era of unrestrained "general warrants" by the British.[85] After "no major Fourth Amendment cases for 100 years,"[86] however, the Court heard

77. Kerr, *supra* note 76, at 481.
78. Bronshteyn, *supra* note 36, at 470–71
79. *Id.* at 470.
80. *See id.* at 479; *see, e.g.*, Riley v. California, 573 U.S. 373, 375–97 (2014); Kyllo v. United States, 533 U.S. 27, 40 (2001).
81. Carpenter v. United States, 138 S. Ct. 2206, 2213–16 (2018).
82. U.S. CONST. amend. IV.
83. Ferguson, *supra* note 32, at 566.
84. Camara v. Mun. Ct. of S.F., 387 U.S. 523, 528 (1967); *see, e.g.*, Dow Chemical Co. v. United States, 476 U.S. 227, 240 (1986) (Powell, J., dissenting).
85. Ferguson, *supra* note 32, at 596; *see also* Julia R. Shackleton, *Alexa, Amazon Assistant or Government Informant?*, 27 U. MIAMI BUS. L. REV. 301, 327 (2019).
86. Ferguson, *supra* note 32, at 568.

Boyd v. United States[87] and extended constitutional protection from physical searches to the right of "personal liberty and private property."[88] The Court held that the law protects citizens from being compelled to produce private papers (in this case business invoices) and noted its equivalency to witnessing against oneself as "condemned in the Fifth Amendment."[89] Yet, for years, Fourth Amendment protection would be grounded in the notion of physical trespass of one's property. For example, in *Olmstead v. United States*, the Court found no search in electronic eavesdropping where telephone conversations were intercepted by wiretapping lines outside of one's home.[90] But by 1967, interpretation swung to protecting "people, not places."[91] In *Katz v. United States*, electronic eavesdropping occurred when federal agents attached a microphone and recording device to a public telephone booth.[92] The Court found that when shutting the door and placing a call, a caller manifests a subjective expectation of privacy in the content of their call.[93] In overruling *Olmstead*,[94] the Court made clear that physically trespassing with the device was no longer required for constitutional protection.[95]

Since *Katz*, the Court has further defined Fourth Amendment protection while largely responding to new technologies and the innovative opportunities they present for government surveillance and investigation.[96] These cases have ranged from telephone wiretaps and pen registers,[97] to thermal imagers,[98] Global Positioning System (GPS) devices,[99] and most recently, cell phones.[100] In general, two lines of cases have emerged. One addresses reasonable expectations of privacy of individuals in the home, and the other addresses the expectations of privacy when information is turned over to third parties.[101]

87. Boyd v. United States, 116 U.S. 616 (1886).
88. *Id.* at 630.
89. *Id.* at 633; Shackleton, *supra* note 85, at 315.
90. Olmstead v. United States, 277 U.S. 438, 466 (1928).
91. Katz v. United States, 389 U.S. 347, 351 (1967).
92. *Id.* at 348.
93. *Id.* at 361.
94. *Id.* at 353.
95. *Id.*
96. Bronshteyn, *supra* note 36, at 471.
97. Smith v. Maryland, 442 U.S. 735, 736 (1979).
98. Kyllo v. United States, 533 U.S. 27, 29 (2001).
99. United States v. Jones, 565 U.S. 400, 402 (2012).
100. Riley v. California, 573 U.S. 373, 378 (2014); Carpenter v. United States, 138 S. Ct. 2206 (2018).
101. Murphy, *supra* note 56, at 792–93.

B. Applying *Carpenter*

A 2018 landmark Supreme Court decision provides the most recent interpretation of applying Fourth Amendment doctrine to new technology and offers the clearest framework yet for how to treat smart home data and communications. In *Carpenter v. United States*,[102] the Justices were confronted with the question of "how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals."[103] In doing so, the Court considered how the expectation of privacy and third-party doctrine applies to the privacy of historical cell-site location information (CSLI).[104] CSLI is generated when a phone communicates with a cell tower. Wireless carriers collect and store CSLI for their own business purposes.[105] In this case, the government had obtained a week's worth of Timothy Carpenter's mobile phone location records from several wireless carriers without a warrant.[106] As part of a criminal investigation, FBI agents used the phone records to create maps showing that certain phones had been in the vicinity of a string of robberies.[107] To obtain the records, prosecutors relied on a provision of the Stored Communications Act, which does not require probable cause.[108] But the Court held that government acquisition of cell-site location records constitutes a Fourth Amendment search.[109]

In writing for the majority, Chief Justice Roberts first emphasized the evolution of Fourth Amendment doctrine. Chief Justice Roberts reminded the Court that common law trespass and property rights are no longer the sole measure of a constitutional violation;[110] protection is extended to "certain expectations of privacy as well."[111] *Katz v. United States*[112] expanded the conception of the Fourth Amendment to state that when an individual "seeks to preserve [something] as private," and his expectation of privacy is "one that society is prepared to recognize as

102. 138 S. Ct. at 2206.
103. *Id.* at 2216.
104. *Id.* at 2216–17.
105. *Id.* at 2211–12.
106. *Id.* at 2212.
107. *Id.* at 2212–13.
108. 18 U.S.C. § 2703(d). The Stored Communications Act allows the government to compel the disclosure of telecommunications records when "specific and articulable facts show that there are reasonable grounds to believe" that such records "are relevant and material to an ongoing criminal investigation." *Id.*
109. *Carpenter*, 138 S. Ct. at 2223.
110. *Id.* at 2213 (citing Soldal v. Cook County, 506 U.S. 56, 64 (1992)).
111. *Id.* (citing Katz v. United States, 389 U.S. 347, 351 (1967)).
112. *Katz*, 389 U.S. at 347.

'reasonable,'" then an official intrusion into that private sphere would qualify as a search that requires a warrant supported by probable cause.[113] Indeed, this two-prong test[114] would provide the threshold for analyzing subsequent Fourth Amendment searches.

Chief Justice Roberts then explained how changes in technology now necessitate a more nuanced approach rather than a "mechanical interpretation" of the Fourth Amendment.[115] Chief Justice Roberts noted that the development of surveillance tools has enhanced the government's ability to "encroach upon areas normally guarded from inquisitive eyes."[116] Chief Justice Roberts pointed to *Kyllo v. United States*, in which the Court held that the use of a thermal imager to detect heat radiating from the defendant's home constituted a search, saying that any other conclusion would leave homeowners "at the mercy of advancing technology."[117] Likewise, in *Riley v. California*,[118] the Court recognized the "immense storage capacity" of modern cell phones in holding that police officers must generally obtain a warrant before searching the contents of a phone.[119] In much the same way, smart home data would also likely enjoy this same evolving Fourth Amendment protection, given the enhanced technological capabilities of smart devices akin to smart phones.

Nonetheless, Chief Justice Roberts acknowledged that CSLI does not "fit neatly under existing precedents,"[120] and he wrote that it lies instead at the "intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake."[121] In this sense, the *Carpenter* Court created a new approach for similar "cases that do not fit neatly into the existing Fourth Amendment framework."[122] In *Carpenter*, the Court examined a "person's expectation of privacy in his physical location and movements," as well as privacy expectations under the third-party doctrine, whereby CSLI is shared with cellular carriers.[123] In this sense, smart home data would also likely be treated under this similar, evolving intersection of precedents. Although geolocation cases in particular would not directly apply to smart home technology because

113. *Id.* at 351, 361.
114. *Id.* at 361 (Harlan, J., concurring).
115. *Carpenter*, 138 S. Ct. at 2214 (citing Kyllo v. United States, 533 U.S. 27, 35 (2001)).
116. *Id.*
117. *Id.*
118. Riley v. California, 573 U.S. 373, 373 (2014).
119. *Id.* at 393, 401.
120. *Carpenter*, 138 S. Ct. at 2214.
121. *Id.* at 2214–15.
122. Murphy, *supra* note 56, at 793.
123. 138 S. Ct. at 2214–15.

the devices are generally stationary in nature (aside from voice-assisted features tied to mobile smart phones), the arguments are instructive as they apply to both an expectation of privacy and the third-party doctrine.

1. Expectation of Privacy

In the first line of cases, an expectation of privacy and Fourth Amendment protection is determined in part by the sophisticated nature of the surveillance technology and duration of the monitoring. In particular, the *Carpenter* Court cited *United States v. Jones*[124] where it held that a warrant was required for the placement of a GPS device on a vehicle to monitor its movements. Distinguishing its decision in *United States v. Knotts*,[125] where a simple beeper placed in a car merely augmented police tracking of movements in public, the Court in *Jones* found that the police used "more sophisticated surveillance"[126] to track "every movement"[127] a person makes in a vehicle. Moreover, the Court found that this "longer term GPS monitoring"[128] done in most police investigations "impinges on expectations of privacy."[129] In *Carpenter*, the CSLI required high-level acquisition and constituted several days of data, exceeding a reasonable expectation of privacy.[130] Following this line of reasoning, the acquisition of smart home data and recordings would also require sophisticated techniques, and any police monitoring of smart home devices may similarly extend over many days instead of a single interaction, infringing on an expectation of privacy.

In applying the second prong of the expectation of privacy test, the *Carpenter* Court determined the expectation of privacy in CSLI to be reasonable.[131] Chief Justice Roberts looked to *Jones*, where it was considered reasonable for society to expect law enforcement to not secretly monitor and catalogue every movement of an individual.[132] The monitoring of personal cell phone CSLI poses an even greater threat than

124. 565 U.S. 400, 404 (2012).
125. 460 U.S. 276, 282 (1983).
126. *Carpenter*, 138 S. Ct. at 2215.
127. *Id.* (citing 565 U.S. 400, 430).
128. *Id.*
129. *Id.*
130. Chief Justice Roberts notes in a footnote that "we need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search." *Id.* at 2217 n.3.
131. *Id.* at 2219.
132. *Id.* at 2218.

the GPS in *Jones*. In particular, "the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them, his 'familial, political, professional, religious, and sexual associations.'"[133] Moreover, the "retrospective quality of the data here gives police access to a category of information otherwise unknowable."[134] Roberts also cited *Riley* in stating that a cell phone is almost a "feature of human anatomy,"[135] and that without Fourth Amendment protection "[o]nly the few without cell phones could escape this tireless and absolute surveillance."[136] Indeed, while today's smart home devices may not be as indispensable as personal cell phones just yet, the information collected would certainly provide far more intimate details about a user than CSLI. Since these devices are becoming more pervasive, are being used primarily in the home, and (in the case of smart speakers) are collecting complete conversations—including those of unwitting guests—the courts would likely find users to have an expectation of privacy that society would recognize as reasonable.

2. Third-Party Doctrine

The *Carpenter* Court also examined the line of cases dealing with an expectation of privacy associated with the third-party doctrine. Under the third-party doctrine, information that is shared with a third party is not subject to Fourth Amendment protection. For example, in *United States v. Miller*,[137] the Court found no expectation of privacy, and therefore no Fourth Amendment protection, for bank documents such as checks and deposit slips that are shared with a third party, the bank. This remains true "even if the information is revealed on the assumption that it will be used only for a limited purpose."[138] Likewise, in *Smith v. Maryland*,[139] the Court held that there is no expectation of privacy in the phone numbers a person dials because those numbers are revealed to a third party, a telephone company. Therefore, in the case of CSLI, it was

133. *Id.* (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).
134. *Id.* at 2218.
135. 573 U.S. 373, 393 (2014). Indeed, in *Riley*, the Court reasoned that greater protection is needed because essentially a person's entire life can be stored on a cell phone. *Id.* at 393–94. The Court stated that "[M]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. . . . Many of these devices are in fact minicomputers. . . . One of the most notable distinguishing features of modern cell phones is their immense storage capacity." *Id.*
136. *Carpenter*, 138 S. Ct. at 2218.
137. 425 U.S. 435, 442 (1976).
138. *Id.* at 443.
139. 442 U.S. 735, 742 (1979).

argued that an individual's cell-site location information is shared with a third party, their cellular carrier.[140] By extension, this same argument can apply to smart home data that is shared with providers such as Amazon and Google.

But in *Carpenter*, Chief Justice Roberts distinguished CSLI from the precedents of *Miller* and *Smith*, pointing to the involuntary nature of the information sharing. He noted that "[w]hen Smith placed a call, he 'voluntarily conveyed' the dialed numbers to the phone company by 'expos[ing] that information to its equipment in the ordinary course of business.'"[141] Yet, with CSLI, that information "is not truly 'shared' as one normally understands the term."[142] "[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up."[143] Chief Justice Roberts reasoned that a user does not voluntarily assume the risk of sharing the data because short of "disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[144] Chief Justice Roberts explained that this decision is narrow and neither changes *Smith* and *Miller*, nor "call[s] into question conventional surveillance techniques and tools, such as security cameras . . . [or] business records that might incidentally reveal location information."[145] So would the sharing of smart home data with Amazon and Google be considered voluntary under *Miller* and *Smith*, or involuntary under *Carpenter*? The courts may determine that the use of smart home devices is more voluntary than involuntary since users do not rely on any particular device, such as a smart TV, refrigerator, or vacuum, as much as they do their mobile smart phones. But just as smart phones were once a novelty, it is predicted that smart home devices could soon become equally indispensable to their users, placing smart home technology outside the scope of the third-party doctrine and affording it Fourth Amendment protection.

Another reason for not extending the third-party doctrine to CSLI was the enhanced collection capabilities of cellular carriers. "There 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."[146] Chief

140. *Carpenter*, 138 S. Ct. at 2220.
141. *Id.* at 2216 (citing *Smith*, 442 U.S. at 736).
142. *Id.* at 2220.
143. *Id.*
144. *Id.*
145. *Id.*
146. *Id.* at 2219.

Justice Roberts pointed to the "seismic shifts in digital technology"[147] that have made possible the tracking of information for "years and years."[148] And again, the nature and degree of the information revealed to these third parties is important. Chief Justice Roberts distinguished the limited ability to reveal sensitive information in *Smith* and *Miller* to the lack of "comparable limitations on the revealing nature of CSLI."[149] Such a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years . . . implicates privacy concerns far beyond those considered in *Smith* and *Miller*."[150] Chief Justice Roberts concluded that because of the "deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[151] This judicial sentiment suggests that the smart home would also escape the third-party doctrine and be constitutionally protected because of the breadth, depth, and reach of its data and communications, which may reasonably be deemed even greater than that associated with CSLI.

3. Other Considerations

While *Carpenter* provides a good framework for how a smart speaker privacy case will be treated, there are other features unique to smart home devices and the law that deserve consideration. In the first place, the Fourth Amendment protects the sanctity of the home,[152] which is precisely where smart home devices are located and used. Unlike CSLI smart home data and communication is generated from within its owner's home—which may even include places traditionally associated with the highest degrees of privacy expectation and hence protection, namely the bedroom or bathroom. As mentioned earlier, information collected by smart home devices may be highly intimate or sensitive, in part because they are located in the home where such conversations are most likely to occur.

The Supreme Court has long recognized that the Fourth Amendment draws a firm line at the entrance of the home.[153] While that

147. *Id.*
148. *Id.*
149. *Id.*
150. *Id.* at 2220.
151. *Id.* at 2223.
152. Kyllo v. United States, 533 U.S. 27, 40 (2001).
153. Payton v. New York, 445 U.S. 573, 589–90 (1980).

line is not absolute,[154] intrusions into the home, such as through acts of wiretapping, eavesdropping, or voyeurism, are generally found to be unlawful when they are committed with the aided eye or ear.[155] For example, if one merely hears a conversation loudly emanating from a home while standing outside on a public sidewalk, there would be no privacy violation because the speakers would have no reasonable expectation of privacy in that conversation.[156] However, if technology that is not in general public use is needed and used to capture a conversation heard only within the home, a privacy violation would likely occur, including a Fourth Amendment violation if the receiver is the government, such as law enforcement officials.[157]

Kyllo v. United States once again provides guidance here.[158] In *Kyllo*, the Court held that law enforcement use of a thermal imaging device to monitor the inside of a home was unconstitutional, saying that the home's sanctity cannot be breached by technology that is not in general public use.[159] In this case, law enforcement used a thermal imager to scan Kyllo's house from a van across the street to determine whether or not Kyllo was growing marijuana in his home using high-intensity lamps that generate a lot of heat.[160] The Court found that when "the Government uses a device that is not in general public use, to explore the details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[161] Certainly, if communication over a smart speaker, for example, was not merely overheard through an open window but was bugged, wiretapped, or otherwise captured using sophisticated technical means, there would be an illegal search. The expectation of privacy would be great.

Another factor to consider is the type of information involved. CSLI is limited to location data, but smart home data might consist of complete conversations and room sounds taken from a smart speaker or real-time video images taken from a pet camera or video doorbell. This distinction between the conduct of a communication and the contents of

154. Aerial surveillance of private homes and surrounding areas does not necessarily constitute a search if there is no reasonable expectation of privacy that society is willing to recognize as reasonable. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 450 (1989); California v. Ciraolo, 476 U.S. 207, 211 (1986).

155. *Kyllo*, 533 U.S. at 31–32.

156. *Id.* at 32–33.

157. *Id.* at 34.

158. *Id.* at 29.

159. *Id.* at 40.

160. *Id.* at 29–30.

161. *Id.* at 40.

the communication is legally significant. *Katz* and *Smith* highlight these differences. In *Katz*, the Court found that when FBI agents attached a listening device to the outside of a public phone booth to monitor Katz's conversations,[162] Katz had an expectation of privacy in the contents of his telephone call. Later in *Smith*, however, the Court found no expectation of privacy in the telephone numbers that Smith dialed when the police had the telephone company use a pen register to record the numbers he dialed from his home.[163] In fact, the Court found that even though Smith may have intentionally called from the privacy of his home in order to keep the *contents* of his conversation private, his *conduct* (placing the call) was not calculated to preserve the number he dialed.[164] *Smith* distinguished conduct from content without diminishing the landmark holding in *Katz* that established that the Fourth Amendment protects the contents of a traditional telephone call.[165] Given that at least some smart home devices produce information that could be viewed as comparable to the contents of a telephone call, their privacy protection would likely prevail under *Katz*.

Finally, the government cannot access records by relying on the statutory authority of only a court order or subpoena where a legitimate privacy interest is protected by the Fourth Amendment—a warrant is required.[166] In *Carpenter*, the FBI seized Carpenter's cell-site records by relying on the Stored Wire and Electronic Communications Act,[167] which addresses the unlawful access to stored communications and the voluntary and required disclosure of customer communications or records. The Act authorizes the government to compel from a "remote computing service" the disclosure of the contents and records of a wire or electronic communications through a warrant,[168] an administrative subpoena,[169] or a court order.[170] In *Carpenter*, a court order was used, which only required the government "to show 'reasonable grounds' for believing that the records were 'relevant and material to an ongoing investigation.'"[171] The Court found this standard to be a "'gigantic' departure from the probable cause rule" of a warrant,[172] with Chief

162. Katz v. United States, 389 U.S. 347, 348 (1967).
163. Smith v. Maryland, 442 U.S. 735, 741 (1979).
164. *Id.* at 743.
165. *Id.* at 741.
166. Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018).
167. 18 U.S.C. §§ 2701–13.
168. *Id.* §§ 2703(a), (c)(1)(A).
169. *Id.* § 2703(b)(1)(B)(i).
170. *Id.* §§ 2703(b)(1)(B)(ii), (c)(1)(B).
171. 138 S. Ct. at 2221 (quoting 18 U.S.C. § 2703(d)).
172. *Id.*

Justice Roberts arguing that law enforcement agents could subpoena records "for no reason other than 'official curiosity.'"[173] Having found the acquisition of CSLI to be a search, the Court concluded that the government must obtain a warrant supported by probable cause before acquiring the records held by a third party.[174] For this reason, acquisition of smart home data by the government could also require a warrant. A concern is that regardless of whether a warrant, subpoena, or court order is used, subscribers or customers may not be notified of the content's disclosure,[175] and no cause of action can be taken against a provider for disclosing the information to the government.[176] Nonetheless, if a constitutionally protectable privacy interest in smart home data is found, at least a warrant with the higher standard of probable cause must be obtained.[177] Indeed, at least one scholar has argued that there should be an even stricter standard than a warrant because of the "granularity" and "quantum" of personal data produced by smart devices in the home.[178]

III. PRIVACY RIGHTS GOING FORWARD

Carpenter was considered a "rare case" in finding a legitimate privacy interest in CSLI records held by a third party.[179] Now courts will need to further examine, interpret, and apply the constitutional protections of the Fourth Amendment, so as Justice Brandeis once explained: the "progress of science" does not erode Fourth Amendment protections.[180] Here, progress is the development of powerful smart tools available to citizens and law enforcement that carry with them privacy risks necessitating constitutional protection. At the same time, courts will need to further grapple with how to apply the precedents of an expectation of privacy, the third-party doctrine, and the *Carpenter* decision when addressing newer technologies, such as today's smart home.

The decision in *Carpenter* was narrow at 5-4 with each of the four dissenting Justices filing separate opinions which, under a newly aligned

173. *Id.* at 2222.
174. *Id.* at 2221.
175. 18 U.S.C. § 2703(b)(1)(A)–(B).
176. *Id.* § 2703(e).
177. *Carpenter*, 138 S. Ct. at 2221.
178. Murphy, *supra* note 56, at 824 (citing Bernard Bell, *Too Smart by Half?:* Naperville Smart Meter Awareness v. City of Naperville, YALE J. REG.: NOTICE & COMMENT (Nov. 6, 2018), http://yalejreg.com/nc/too-smart-by-half-naperville-smart-meter-awareness-v-city-of-naperville/).
179. 138 S. Ct. at 2222.
180. Olmstead v. United States, 277 U.S. 438, 473–74 (1928).

Supreme Court, may be persuasive when analyzing and distinguishing a future Fourth Amendment case involving smart home devices.[181] Indeed, the dissenting opinions suggest that cases could turn on whether users are seen as having a property right in, or ownership control of, their data records and communications that third-party providers collect in the provision of their service. For example, Justice Kennedy dissented, arguing that the property-based conceptions of the Fourth Amendment must still apply, saying there is no expectation of privacy in records the defendants have "no reason to believe . . . were owned or controlled by them."[182] Kennedy stated that the third-party doctrine should therefore apply because CSLI is no different from other provider business records the government can lawfully obtain by compulsory process.[183] Justice Thomas also stated that the matter should turn on whose property was searched,[184] and he criticized *Katz*, arguing that the reasonable expectation of privacy test has no foundation in the text of the Fourth Amendment[185] whose focus has been mistakenly shifted from property to privacy.[186] Justice Gorsuch also suggested revisiting a more traditional property rights approach to the Fourth Amendment but argued that, in doing so, Fourth Amendment protections may actually be enhanced.[187] He contended that Fourth Amendment interests in records given to a third party may be extinguished when applying *Smith* and *Miller*, but preserved when finding a property right in records.[188] Furthermore, complete ownership or exclusive control of property may not be necessary to assert a Fourth Amendment right,[189] and entrusting a third party with one's data would not necessarily mean losing all Fourth Amendment protections in it.[190] Thus, if evolving Fourth Amendment doctrine returns to a property rights approach, a property right in the data generated by smart home devices would need to be advanced. While CPM theory would posit that both parties become co-owners of an information disclosure,[191] a property argument could be

181. *See* Aaron Dalton, Carpenter v. United States*: A New Era for Protecting Data Generated on Personal Technology, or a Mere Caveat?*, 20 N.C. J. L. & TECH., 1, 19–20 (2018) (arguing that the *Carpenter* Court failed to articulate a clear standard for applying its decision to future technologies).
182. *Carpenter*, 138 S. Ct. at 2228 (Kennedy, J., dissenting).
183. *Id.* at 2224.
184. *Id.* at 2235 (Thomas, J., dissenting).
185. *Id.* at 2236.
186. *Id.* at 2241.
187. *Id.* at 2268–69 (Gorsuch, J., dissenting).
188. *Id.* at 2272.
189. *Id.* at 2269.
190. *Id.* at 2268.
191. Petronio & Durham, *supra* note 51, at 338.

made in pointing to the generating and controlling of one's personal data as a necessary function of living in a "political, economic, and social world" that requires data sharing.[192] Moreover, if such rights are found for CSLI, or even legislated for comparable stored communications and records, protection of smart home data could prevail under a property rights conception.

The *Carpenter* Court certainly acknowledged that more work needs to be done.[193] For example, while the Court found a reasonable expectation of privacy, Justice Gorsuch explained that "courts now must conduct a *second Katz*-like balancing inquiry, asking whether the fact of disclosure to a third party outweighs privacy interests in some 'category of information' disclosed."[194] Assigning values to different categories of seized information could be difficult and troubling, though, with Justice Gorsuch noting that seven days of CSLI now receives protection but a lifetime of bank records does not.[195] Still, when compared to location records, smart technologies and their use in the home could neatly comprise a "category" of information deserving of protection.

The treatment of the third-party doctrine is where the *Carpenter* Court made its most radical departure, though, and where further elucidation and understanding is needed as Fourth Amendment jurisprudence is reshaped. The third-party doctrine has perhaps become the "most reviled Fourth Amendment canon."[196] Voluntary disclosure decisions have garnered the most criticism of Fourth Amendment cases,[197] and scholars have even recognized the doctrine as "one of the most serious threats to privacy in the digital age."[198] With its relatively untouched roots dating back to 1979, the third-party doctrine has been called outdated.[199]

Carpenter struck a major blow to the reach of the doctrine by limiting its application and declining to extend *Smith* and *Miller* to the third-party collection of CSLI. Again, until *Carpenter*, courts had uniformly and "mechanically"[200] applied the third-party doctrine to all information voluntarily disclosed and did not necessarily consider the

192. *See, e.g.*, Shackleton, *supra* note 85, at 326.
193. 138 S. Ct. at 2267 (Gorsuch, J., dissenting).
194. *Id.*
195. *Id.*
196. Bronshteyn, *supra* note 36, at 487.
197. *Id.* (quoting Clark D. Cunningham, *A Linguistic Analysis of the Meanings of "Search" in the Fourth Amendment: A Search for Common Sense*, 73 IOWA L. REV. 541, 580 (1988)).
198. *Id.* (quoting Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005)).
199. Shackleton, *supra* note 85, at 322.
200. 138 S. Ct. at 2219.

privacy interest in those records.[201] As Justice Alito stated, "until today—defendants categorically had no 'reasonable expectation of privacy' and no property interest in records belonging to third parties."[202] But it is important to note that *Carpenter* took care to retain the third-party doctrine and did not overrule *Smith* and *Miller*. With the reach of *Smith* and *Miller* now less clear, courts will need to determine whether and how to extend *Smith* and *Miller* to new cases before them while also applying *Carpenter*.

Carpenter limited the third-party doctrine and distinguished *Smith* and *Miller* in ways that deserve further consideration and perhaps new construction. In the first place, the reasonable expectation of privacy standard could be clarified to prevent unrestrained government surveillance and access. The notion of liberty and autonomy set forth in *Katz* is not protected when a reasonable expectation of privacy is found, and people are generally unaware that their communications and personal data are being collected and recorded.[203] The standard for consent needs to be raised from *Smith* because most people do not read their various service providers' lengthy terms of use agreements or understand that their information could be shared with government agencies. Again, people will tend to self-disclose despite warnings, not understanding the extent and risks of sharing their personal information when weighing the benefits of using a technology.[204] *Carpenter* narrowed the conception of meaningful consent for CSLI by explaining that one's cell phone location information is transmitted automatically, without an affirmative act on the part of the user and is a pervasive necessity for participation in modern society.[205] A stricter standard of meaningful consent should also apply to smart home devices and comparable smart technologies. Likewise, a higher standard for disclosure, one that society would deem as reasonable, is needed due to the intimate nature of smart home data and the mosaic effect where digital information produces a comprehensive "dossier"[206] of one's life. The magnitude of the disclosures renders such data as more deserving of privacy protection than those of *Smith* and *Miller*.

Another area warranting attention is the way in which *Carpenter* distinguished *Smith* and *Miller* based on the assumption of risk taken

201. Murphy, *supra* note 56, at 794 (citing Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976)).
202. *Carpenter*, 138 S. Ct. at 2255 (Alito, J., dissenting).
203. Shackleton, *supra* note 85, at 322.
204. Robinson, *supra* note 48, at 11.
205. Bronshteyn, *supra* note 36, at 491.
206. *Carpenter*, 138 S. Ct. at 2220.

when sharing information with a third party. *Carpenter* took a narrow view of voluntariness, finding that an individual simply carrying a cell phone does not voluntarily assume the risk of constant monitoring as they would when making a bank deposit or dialing numbers on a phone.[207] Here, the elements of meaningful consent would be weighed. Yet the assumption of risk approach arguably provides a weak basis for remaking Fourth Amendment jurisprudence in the modern era.[208] On the one hand, its rationale is circular; if the law protected the disclosed information, then there would be no risk to assume.[209] A conflict also occurs when considering the pervasiveness of the technology as reasoned by the *Carpenter* Court as a measure of meaningful consent.[210] In this sense an individual assumes the risk when adopting a new technology and could be denied Fourth Amendment protection until some level of widespread adoption is met.[211] As a result, some scholars suggest abandoning the assumption of risk barrier to Fourth Amendment protection and folding the voluntary disclosure analysis into the reasonable expectation of privacy test.[212] In this way, the courts would rethink the third-party doctrine and return to the *Katz* expectation of privacy doctrine, applying its analysis even when the information is shared with a third party.[213] In this sense, the courts would look less at whether users voluntarily conveyed their communication and more at how smart home services have become a requisite part of daily life.

IV. CONCLUSION

While no laws currently address smart home privacy, evolving Fourth Amendment protection should apply to smart home technology in this time of rapid technological advancement and opportunity for infringement. Although the decision in *Carpenter* provides the latest guidance for analysis, courts will need to further address the precedents of *Smith* and *Miller* and distinguish the privacy interests associated with smart home data from other types of digital information and data, such as CSLI. Smart home technologies will need to be scrutinized for their

207. *Id.*
208. Bronshteyn, *supra* note 36, at 492.
209. *Id.* at 488.
210. *Id.* at 493.
211. *Id.* at 494.
212. *Id.* at 487; *see also* Gabriel Broshteyn, Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1945 (2017).
213. *Broshteyn*, *supra* note 212, at 1945.

potential to reveal a mosaic of deeply personal information that is generated from the sanctity of the home, oftentimes automatically and with broad reach, and aggregated to create a remarkably comprehensive picture of the lives of smart home occupants. The expectation of privacy test will need to continue to evolve to address the features and use of smart technology, while the third-party doctrine should be re-evaluated, rethinking the assumption of risk standard, meaningful consent, and the voluntariness of the data disclosure to third-party service providers.

As more smart devices appear in homes, it is certain that law enforcement agencies will increasingly turn to them as important investigative tools, producing valuable data. Courts will need to continue to balance the interests of government with the fundamental privacy rights of citizens, but also recognize a Fourth Amendment right in smart home data, therefore, requiring law enforcement officials to at least obtain a warrant based on probable cause before obtaining smart home data and communications from third-party providers. Indeed, the rise of smart home technology presents new challenges for Fourth Amendment jurisprudence. Treatment of the smart home will need to be smart and its privacy protections guaranteed.