University of Miami Race & Social Justice Law Review

Volume 10
Issue 2 *Spring 2020*

Article 3

April 2020

Smart Homes: The Next Fourth Amendment Frontier

Christina A. Robinson

Smart Homes:
The Next Fourth Amendment Frontier

Christina A. Robinson*

Under the third-party search doctrine, an individual does not have a reasonable expectation of privacy in information he or she voluntarily discloses to third parties. "Always on" in-home technology creates recordings of unsuspecting consumers in their most intimate spaces and sends them to third party companies and their affiliates, which makes this information subject to warrantless search by law enforcement under the third-party search doctrine. The third-party search doctrine is ill-suited to the digital age, where consumers are routinely required to volunteer information to third parties in order to access digital content. This Note suggests that a warrant should be required where the government attempts to search "always on" in-home technology.

---

* This Note is dedicated to the people who made it possible for me to become a lawyer. To my parents, Professor Thomas Robinson and Professor Christine Robinson, thank you for loving me unconditionally, teaching me the value of education and integrity, and supporting me in everything I do. To my siblings, Sita Whitaker-Robinson and "TC" Robinson, thank you for being my guiding lights and always looking out for me as only older siblings can. I am particularly grateful to my girlfriend, Megan Cheney, without whose wisdom and patience this Note would never have been published. Special thanks to Professor Tamara Lave, who introduced me to many of these cases and challenged me throughout law school to become the best version of myself. Special thanks also to Assistant Dean Marni Lennon who inspired me to use my law degree in service of others and without whose friendship and mentorship I would not be where I am today.

I. INTRODUCTION

> The telescreen received and transmitted simultaneously. Any sound that [a person] made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.[1]

Government surveillance is omnipresent in George Orwell's famous book, *1984*. In the novel, home appliances simultaneously deliver digital content to the protagonist, Winston Smith, and surveil his every move.[2] As a result, Winston knows he must be ever vigilant of his words and actions, even inside his own home. Orwell's novel was written in 1949 as a glimpse into a potentially totalitarian future,[3] but over thirty years after the year 1984 how far away are we from Orwell's dystopia becoming our reality?

The scary truth may be that new "always on" in-home technology may be bringing us closer to Orwell's world than we realize. The Amazon Echo Dot controversy in two murder investigations provides an easy example. The Echo Dot is a relatively cheap smart home appliance—or, as you might call it, a Christmas present. The device is designed to remain powered on, always listening for the command word, "Alexa," which allows the user to control music and command smart home devices using just his or her voice.[4] After voice activation the device records sound in

---

1 GEORGE ORWELL, 1984 4 (1949).

2 *Id.*

3 Colin Marshall, *George Orwell Explains in a Revealing 1944 Letter Why He'd Write 1984*, OPEN CULTURE (Apr. 17, 2018), http://www.openculture.com/2014/01/george-orwell-explains-in-a-revealing-1944-letter-why-hed-write-1984.html.

4 Eliott C. McLaughlin & Keith Allen, *Alexa, Can You Help with This Murder Case?*, CNN (Dec. 28, 2018), http://www.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd.

the area around it for brief durations, and these recordings are stored by Amazon.[5]

Two murder investigations in which the government requested that Amazon release recordings made by the Echo Dot inside the suspects' homes raise an important question: Will the Echo Dot and similar technology lead to the erosion of Fourth Amendment protection inside the home? This Note discusses the implications of "always on" in-home technology on Fourth Amendment jurisprudence. Part II expounds on the privacy implications posed by the Echo Dot and similar "always on" in-home technology. Part III explains the current status of Fourth Amendment jurisprudence on the issue. Part IV provides suggested solutions, and Part V concludes with final thoughts.

II. STATEMENT OF THE PROBLEM

A. Alexa, Set an Alarm for 2020

Smart devices are nearly ubiquitous in modern society. They do everything from helping us check the weather to reading us the morning news. A report by the Consumer Technology Association estimates that the majority of households in the United States, a whopping sixty-nine percent or 83 million households, own at least one smart home device; eighteen percent or 22 million households own more than one smart device.[6] Berg Insight, a Swedish research firm, estimates that 63 million American homes will qualify as "smart" homes by 2022.[7] Over twenty-five percent of American households owned a smart home speaker in 2019, and that number is growing rapidly.[8] The Amazon Echo and the Google Home are the most common smart speakers with the Apple HomePod and other smart speakers close behind.[9] The United States has

---

5 *Id*.

6 Chuck Martin, *Smart Home Technology Hits 69% Penetration in U.S.*, MEDIAPOST (Sept. 30, 2019), https://www.mediapost.com/publications/article/341320/smart-home-technology-hits-69-penetration-in-us.html.

7 Patrick Austin, *What Will Smart Homes Look Like 10 Years From Now?*, TIME (July 25, 2019), https://time.com/5634791/smart-homes-future/.

8 Sarah Perez, *Over A Quarter of US Adults Now Own a Smart Speaker Typically an Amazon Echo*, TECHCRUNCH (Mar. 8, 2019), https://techcrunch.com/2019/03/08/over-a-quarter-of-u-s-adults-now-own-a-smart-speaker-typically-an-amazon-echo/.

9 *Id*.

the highest market penetration for smart speakers of any other country in the world followed by China and the United Kingdom.[10]

But how do these devices work? With seven microphones, the Amazon Echo Dot, like other "always on" technology, voice-activates when it hears its command word, "Alexa."[11] The device is equipped with sensors to hear users from any direction for up to twenty feet.[12] When the Echo Dot is activated a blue light appears, and a tone can be heard that indicates the device is ready to make a user query.[13] After hearing the command word, the Echo Dot creates a recording of the user query and any sound around it.[14] Once the command and any accompanying sounds have been recorded, they are saved on Amazon's servers and can be reviewed (and deleted) manually by the user.[15] Importantly, even though the Echo Dot is not recording when the device has not been activated with the command word, it is still on and "always listening" for the command word at all times.[16]

The Amazon Echo Dot and other smart speakers are easy examples of "always on" in-home technology, but "always on" devices that have the ability to record in a home can and do come in many forms. Other "always on" devices that can create recordings inside a home include the Google Chrome browser, the Xbox Kinect, the Samsung Smart TV, and Mattel's Hello Barbie.[17] All of these devices save audio clips immediately before and during user queries.[18]

---

10 Shanhong Liu, *Smart Home Voice Assistants Installed Base Share 2017-2019, by Country*, STATISTA (Aug. 9, 2019), https://www.statista.com/statistics/878650/worldwide-smart-speaker-installed-base-by-country/.

11 McLaughlin, *supra* note 4.

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

13 Raphael Davidian, *Alexa and Third Parties' Reasonable Expectation of Privacy*, AM. CRIM. L. REV. ONLINE 58, 59–60 (2017), http://www.americancriminallawreview.com/files/5114/9515/4188/ALEXA_AND_THIRD_PARTIES_REASONABLE_EXPECTATION_OF_PRIVACY_FINAL.pdf.

14 Mele, *supra* note 12.

15 Davidian, *supra* note 13, at 58.

16 *Id*. at 59. Indeed, that is why this technology is said to be "always on." It is also worth noting that the device may accidentally be triggered to record by mistake. For example, if someone in the vicinity says the name "Alex," the device may activate and trigger a recording.

17 Letter from Marc Rotenberg et al., Exec. Dir., Elec. Privacy Info. Ctr., to Att'y Gen. Lynch & Chairwoman Ramirez, 3 (July 10, 2015), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf.

18 Arielle M. Rediger, *Always-Listening Technologies: Who Is Listening and What Can Be Done About It?*, 29 LOY. CONSUMER L. REV. 229, 231 (2017).

Differences in software allow some of these devices even to record audio clips of their surroundings when queries are not being made.[19] For example, in 2015 Google conceded that its Chrome browser contained code that regularly recorded private communications by turning on a microphone that was actively listening to a user's room without the user's knowledge or consent.[20] Similarly, the Xbox Kinect tracked users' gestures, heartbeats, and facial expressions when it was turned on. But even when turned off, the Xbox Kinect monitored conversations taking place around it.[21] The Samsung TV routinely recorded private consumer communications, both related and unrelated to the user query, and sent the recordings to its third-party voice-to-text processor without encryption.[22] In fact, when information surfaced in 2015 that Samsung's voice-to-text processing sent users' private communications to third parties, the Electronic Privacy Information Center filed a complaint with the Federal Trade Commission against Samsung, alleging violations of consumer privacy and wiretapping laws.[23] By far, the most disturbing of the in-home recording devices is the Hello Barbie, which used a built-in microphone to record and transmit information gathered through conversations with children to its toy conglomerate, Mattel, to analyze the child's likes and dislikes.[24]

Many consumers seem to be shocked to find out that their private communications are being recorded by the devices in their homes.[25] The Electronic Privacy Information Center eloquently laid out concerns about the privacy implications of these "always on" devices and others in a letter to Attorney General Lynch and Chairwoman Ramirez in July 2015:

> Americans do not expect that the devices in their homes will persistently record everything they say. By introducing 'always on' voice recording into ordinary consumer products such as computers, televisions, and toys, companies are listening to consumers in their most private spaces. It is unreasonable to expect consumers to

---

19 Letter from Marc Rotenberg et al., *supra* note 17, at 2–5.

20 *Id*. at 2.

21 *Id*. at 3.

22 *Id*.

23 *Id*. at 1; Mike Snider, *FTC: Vizio Smart TVs Spied on What Viewers Watched,* USA TODAY (Feb. 7, 2017), https://www.usatoday.com/story/tech/talkingtech/2017/02/06/vizio-pay-22m-smart-tv-data-gathering/97553144/. The Federal Trade Commission has not announced any action on the complaint as of this writing, but Samsung did issue a statement after the FTC complaint was filed saying that the voice-recognition feature was intended to enhance the user experience and it could be disabled.

24 Letter from Marc Rotenberg et al., *supra* note 17, at 2.

25 *Id*. at 3.

> monitor their every word in front of their home electronics. It is also genuinely creepy.[26]

But if consumers are shocked to find out that these recordings are being made at all, how might they feel if they knew the recordings could also be turned over to law enforcement?

B. Alexa, Can You Solve This Murder Mystery?

On November 22, 2015, police from the Bentonville Police Department in Arkansas found Victor Collins dead in a hot tub at the home of James Bates.[27] After investigators discovered signs of a struggle, Bates was charged with murder.[28] One witness said music had been streaming from the house that night,[29] and during the search of his house police found an Amazon Echo Dot on Bates' kitchen counter.[30] Prosecutors served Amazon with a warrant to obtain all audio recordings made from Bates' Echo Dot in hopes they might contain information about Collins' death.[31] Amazon fought the warrant on the grounds that it was overbroad, stating at first that it "[would] not release customer information without a valid and binding legal demand properly served on us[,]"[32] but ultimately with Bates' consent, Amazon turned the recordings over to prosecutors.[33] After receiving the recordings from the Echo Dot, the main prosecutor, Nathan Smith, began to doubt whether Bates actually committed the murder stating, "I can't stand in front of a jury and ask them to convict someone

---

26 *Id*. at 4–5.

27 Mele, *supra* note 12.

28 *Id.*

29 *Amazon Hands Over Echo 'Murder' Data*, BBC (Apr. 17, 2018), http://www.bbc.com/news/technology-39191056.

30 Mele, *supra* note 12.

31 *See id.*; *see also* Jay Stanley, *The Privacy Threat from Always-On Microphones like the Amazon Echo*, AM. CIV. LIBERTIES UNION (Jan. 13, 2017), https://www.aclu.org/blog/privacy-technology/privacy-threat-always-microphones-amazon-echo?redirect=blog/free-future/privacy-threat-always-microphones-amazon-echo.

32 *Arkansas Prosecutors Drop Murder Case That Hinged On Evidence From Amazon Echo*, NPR (Nov. 29, 2017), https://www.npr.org/sections/thetwo-way/2017/11/29/567305812/arkansas-prosecutors-drop-murder-case-that-hinged-on-evidence-from-amazon-echo. Investigators also used information from a smart water meter on Bates' property to decide to file charges against him. The smart water meter showed a suspiciously large consumption of water being used in the middle of the night.

33 Shona Gosh, *Amazon Handed Over Alexa Recordings to the Police in a Murder Case*, BUS. INSIDER (Mar. 7, 2017), https://www.businessinsider.com/amazon-has-handed-alexa-recordings-to-police-in-an-arkansas-murder-case-2017-3.

beyond a reasonable doubt if I myself have a reasonable doubt [about who committed this crime]."[34] Smith eventually moved to dismiss the case.[35]

Alexa was asked to testify in a second murder investigation in 2017. On January 27, 2017, Jenna Pellegrini and Christine Sullivan were stabbed to death in Farmington, New Hampshire, and Timothy Verrill was charged with their murder.[36] An Amazon Echo Dot was sitting on the kitchen counter, and Judge Steven Houran ordered Amazon to turn over the recordings made from January 27, 2017 to January 29, 2017.[37] Amazon similarly objected to the court order on the basis that it is overbroad and inappropriate.[38] The case went to trial in October 2019 but resulted in a mistrial.[39]

Cases like these raise questions about data from the Amazon Echo Dot and other "always on" in-home devices: Can recordings of our most intimate spaces be turned over to law enforcement officers without our consent—or a warrant?

III. STATEMENT OF THE LAW

A. Privacy Protection Under The Fourth Amendment

The Fourth Amendment to the United States Constitution states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no [w]arrants shall issue but upon probable cause . . . describing the place to be searched, and the . . . things to be seized."[40] In the two centuries following its enactment, the Supreme Court used the text of the Fourth

---

34 Nicole Chavez, *Arkansas Judge Drops Murder Charge in Amazon Echo Case*, CNN (Dec. 2, 2017), https://www.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html?no-st=1526532257.

35 *Id.*

36 Harrison Thorp, *Farmington Double-Murder Trial Postponed till October, could Last Six Weeks*, THE ROCHESTER VOICE (Mar. 13, 2019), https://www.therochestervoice.com/farmington-double-murder-trial-postponed-till-october-could-last-six-weeks-cms-11914.

37 Meagan Flynn, *Police Think Alexa May Have Witnessed a New Hampshire Double Homicide. Now They Want Amazon to Turn Her Over*, WASH. POST (Nov. 14, 2018), https://www.washingtonpost.com/nation/2018/11/14/police-think-alexa-may-have-witnessed-new-hampshire-double-slaying-now-they-want-amazon-turn-her-over/; Perez, *supra* note 8.

38 Perez, *supra* note 8.

39 Kyle Stucker, *'We failed': Mistrial Declared in Double-Murder Case*, FOSTERS.COM (Oct. 31, 2019), https://www.fosters.com/news/20191031/we-failed-mistrial-declared-in-double-murder-case

40 U.S. CONST. amend. IV.

Amendment to craft a set of procedural rules to balance law enforcement needs against individual privacy interests.[41] The warrant clause of the Fourth Amendment mandates that a warrant be issued based on a finding of probable cause by a neutral magistrate.[42] In the absence of a warrant, the government must articulate one of several exceptions to the warrant requirement or risk the inadmissibility of evidence at trial.[43] The fundamental purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials."[44] The Supreme Court is charged with providing the same degree of Fourth Amendment protection today as that afforded when it was adopted,[45] yet Fourth Amendment standards have struggled to keep pace with evolving technology that allows for new government surveillance techniques.[46]

B. The Katz Reasonable Expectation of Privacy Standard

For three decades, government surveillance primarily triggered a Fourth Amendment violation under the "trespass doctrine."[47] The trespass doctrine invokes Fourth Amendment protections when the government physically invades an individual's property without a warrant.[48] For example, in *Silverman v. United States* the Supreme Court found that the government violated the Fourth Amendment by listening to the defendant's private communicates using a "spike mike" placed on the defendant's home-heating duct because the government had physically penetrated his property.[49] However, wiretapping technology capable of recording private conversations in the absence of a physical intrusion was soon introduced.[50] With the advent of this new wiretapping technology, the Supreme Court was forced to rethink the trespass doctrine and articulate a new Fourth Amendment standard.

Initially, in *Olmstead v. United States*, the Supreme Court decided that Fourth Amendment protections did not apply to information obtained by

---

41 *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 536 (2005).

42 *See id*. at 536–37.

43 *See id*.

44 *Camara v. Mun. Ct. of City and City of S.F*., 387 U.S. 523, 528 (1967).

45 *Kyllo v. United States*, 533 U.S. 27, 28 (2001).

46 *See* Jace C. Gatewood, *It's Raining* Katz *and* Jones*: The Implications of* United States v. Jones*–A Case of Sound and Fury*, 33 PACE L. REV. 683, 683–85 (2013).

47 *Id*.

48 *Id*.

49 *Silverman v. United States*, 365 U.S. 505, 510–11 (1961).

50 David A. Harris, *Riley v. California and the Beginning of the End for the Third-Party Search Doctrine*, 18 U. PA. J. CONST. L. 895, 927–28 (2016).

the government in the absence of a physical trespass.[51] However, Justice Brandeis's dissent in *Olmstead* contained seeds of change that would revolutionize Fourth Amendment jurisprudence.[52] Justice Brandeis believed that the Fourth Amendment should be interpreted to keep pace with advances in modern technology, which would create new possibilities for the government to invade individual privacy:

> When the Fourth and Fifth Amendments were adopted, . . . [f]orce and violence were then the only means known to man by which a government could directly effect self-incrimination . . . . But 'time works change, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government . . . to obtain disclosure in court of what is whispered in the closet . . . . The makers of our Constitution . . . . sought to protect Americans in their beliefs, their emotions, and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[53]

In *Katz v. United States*, the Supreme Court overruled the majority's opinion in *Olmstead*, providing that the Fourth Amendment protects individuals even in the absence of a physical intrusion and emphasizing that the Fourth Amendment "protects people, not places."[54] In a concurring opinion, Justice Harlan articulated the standard that continues to govern Fourth Amendment jurisprudence today: A Fourth Amendment violation occurs where law enforcement officials infringe on an individual's subjective expectation of privacy so long as society deems that expectation to be objectively reasonable.[55]

An individual's reasonable expectation of privacy is greatest in his or her home.[56] In *Kyllo v. United States*, the Supreme Court held that the

---

51 *Olmstead v. United States*, 277 U.S. 438, 473–478 (1928).
52 *Id*. at 471–85 (Brandeis, J., dissenting).
53 *Id*.
54 *Katz v. United States*, 389 U.S. 347, 351 (1967).
55 *Id*. at 361 (Harlan, J., concurring).
56 *See* Kerr, *supra* note 41, at 536.

government's use of a thermal-imaging device without a warrant to discover information about the contents of a home, which would be otherwise unknown without a physical intrusion, violated the Fourth Amendment.[57] In an impassioned majority opinion, Justice Scalia emphasized the importance of safeguarding privacy in the home in the face of advances in modern technology.[58] He depicted protection of the home from prying government eyes as the constitutional minimum reasonable expectation of privacy demanded by the Fourth Amendment.[59] Justice Scalia rejected the argument that a failure to discern intimate details about the home prevented a Fourth Amendment violation because "[i]n the home, our cases show, *all* details are intimate details[.]"[60]

C. The Foundations of the Third-Party Search Doctrine

Under the *Katz* test, an individual has no reasonable expectation of privacy in information that he or she voluntarily discloses to third parties under the third-party search doctrine.[61] The third-party search doctrine was first discussed at length in *United States v. Miller*.[62] In *Miller*, the Supreme Court held that the Fourth Amendment does not protect information that has been revealed to third parties, even if the information was revealed on the assumption that it would be used for a limited purpose and that the third party would maintain its privacy.[63] The Court found that Miller had no reasonable expectation of privacy in information he voluntarily disclosed to his bank, and the government could lawfully subpoena his bank records as evidence to be used against him in a criminal prosecution.[64] In other words, "[t]he depositor [assumes] the risk in revealing his affairs to another[] that the information [would] be conveyed" to the government.[65]

The Supreme Court expanded the scope of the third-party search doctrine to include information voluntarily revealed to a phone company

---

57 *Kyllo v. United States*, 533 U.S. 27, 28 (2001).

58 *Id.* at 40 (advocating that it would be foolish to assert that privacy protection under the Fourth Amendment has been unaffected by the advance of technology).

59 *Id*. at 28. By contrast, an individual has no reasonable expectation of privacy in anything in "open fields" or in the plain view of a police officer. In *Oliver v. United States*, 466 U.S. 170, 180 (1984), the Supreme Court held that an individual does not have a reasonable expectation of privacy in information in "open fields," where any member of the public can look.

60 *Kyllo*, 533 U.S. at 37. Importantly, the scope of *Kyllo* is limited to new technology that is not in general public use.

61 *Id*. at 27–28.

62 Harris, *supra* note 50, at 904.

63 *Miller v. United States*, 425 U.S. 435, 443–46 (1976).

64 *Id.* at 445–46.

65 *Id.* at 443.

in *Smith v. Maryland*.[66] The Court reasoned that telephone users have no reasonable expectation of privacy in the outward numbers they dial because users know they must convey information about these numbers to telephone companies, which record this information for legitimate business purposes.[67] The Court distinguished this case from *Katz* by saying that the device employed by the government registered only the numbers dialed, not the contents of the communication.[68] The Court also rejected the argument that the numbers should be entitled to greater protection because they were dialed using a phone from inside the defendant's house because, "[r]egardless of his location, [the] petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call."[69] Citing *Miller*, the Court affirmed that an individual who discloses information to a third party assumes the risk that this information will be provided to law enforcement.[70]

D. Advances in Technology Beget Changing Attitudes Toward the Third-Party Search Doctrine

The Supreme Court readdressed the third-party search doctrine in *United States v. Jones*. The issue in *Jones* was whether the warrantless GPS tracking of a person's car constituted a Fourth Amendment violation. At first, the *Katz* reasonable expectation of privacy test was used in the Supreme Court's decisions involving GPS technology to track suspects.[71] *United States v. Knotts* and *United States v. Karo* were factually similar to *Jones*—all three cases involved government surveillance of the defendant's movements using GPS technology—yet both *Knotts* and *Karo* were decided on the *Katz* reasonable expectation of privacy standard.[72]

But in a surprising turn of events, Justice Scalia, writing for the majority, sidestepped the *Katz* analysis and instead revived the trespass doctrine.[73] Justice Scalia distinguished *Knotts* and *Karo* from *Jones* by

---

66 *Smith v. Maryland*, 442 U.S. 735, 745–46, (1979).
67 *Id.* at 743.
68 *Id.* at 741.
69 *Id.* at 743.
70 *Id.* at 744.
71 The two cases on point are *United States v. Knotts*, 460 U.S. 276, 281 (1983) and *United States v. Karo*, 468 U.S. 705, 714 (1984). In *Knotts*, the Supreme Court held that tracking a defendant by placing a device inside a container he subsequently acquired did not violate the Fourth Amendment because the suspect did not have a reasonable expectation of privacy in his movements on public thoroughfares.[71] On similar facts in *Karo*, the Court held that tracking the defendant when his car was parked inside a private residence did violate his reasonable expectation of privacy.[71]
72 *United States v. Jones*, 565 U.S. 400, 408–10 (2012).
73 *Id*.

saying that a trespass had not occurred in either case because the government placed the tracking device on the property *before* the defendant took possession of it.[74] Justice Scalia made clear that in *Jones* the government placed its tracking device on the defendant's car *after* he had taken possession of it, which made the case ripe for determining it based on the trespass doctrine.[75] Because a car constituted an "effect" under the Fourth Amendment the government physically trespassed onto the defendant's car after he had already taken possession of it, the government violated the Fourth Amendment under the trespass doctrine.[76]

In a famous concurring opinion, Justice Sotomayor agreed that the trespass doctrine was sufficient to decide *Jones*, but she criticized the majority for being shortsighted: "In cases of electronic or other novel means of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance."[77] She then challenged Justice Scalia's notion that people have no reasonable expectation of privacy in the sum of their public movements and laid out several reasons why a *Katz* inquiry was relevant in *Jones*: GPS monitoring allows the government access to information about one's most private associations; GPS tracking information can be stored and mined by the government for years to come; the information is cheap to gather so it evades normal checks on law enforcement officers; and the awareness that the government might be watching chills associational and expressive freedoms.[78] In light of these attributes, she said she would ask "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[79]

Justice Sotomayor then addressed what she believed to be the more important underlying issue in *Jones*, which was the inevitable need to re-evaluate the third-party search doctrine in light of advances in modern technology.[80] She believed that allowing the third-party search doctrine to continue to control would give the government unchecked power over routinely disclosed consumer data:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . This

---

74 *Id*. at 408–09.
75 *Id*.
76 *Id*. at 401.
77 *Id*. at 413–18 (Sotomayor, J., concurring).
78 *Id*.
79 *Id*.
80 *Id.*

> approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[81]

Thus, as Justice Sotomayor noted, the majority in *Jones* effectively left open the question of whether warrantless government surveillance to track the aggregate of an individual's movements in the absence of a physical intrusion would violate the Fourth Amendment. Justice Sotomayor's concurrence indicated that the third-party search doctrine should be re-evaluated in light of advances in modern technology.

E. Legal Trends Move Toward Heightened Protection for Digital Information

Around the same time as *Jones*, some lower courts began to treat digital information with a heightened expectation of privacy. For example, in *United States v. Mitchell*, the Eleventh Circuit held that the detention of the defendant's computer for a duration outside the scope of the warrant violated the Fourth Amendment, especially because a computer hard drive is "the digital equivalent of its owner's home, capable of holding a universe of private information."[82] In *United States v. Warshak*, the Sixth Circuit held that a subscriber maintains a reasonable expectation of privacy in the contents of emails stored, sent, or received through an Internet Service Provider, and the government may only compel the Internet Service Provider to turn over the contents of the subscriber's emails by first obtaining a warrant.[83]

The trend toward treating digital information with a heightened expectation of privacy continued in the United States Supreme Court in 2014 with *Riley v. California*. In *Riley*, the Court took a firm position to protect digital information by imposing a warrant requirement on cell phone searches incident to arrest.[84] The Court stated that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of [other physical items]" because of their immense storage capacity, the tendency that information derived from a

---

81 *Id.*

82 *United States v. Mitchell*, 565 F.3d 1347, 1352 (11th Cir. 2009) (quoting *Kansas v. Rupnick,* 280 Kan. 720, 125 P.3d 541, 552 (2005)).

83 *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).

84 *Riley v. California*, 134 S. Ct. 2473, 2495 (2014).

cell phone search could reveal much more about a suspect's personal life in combination than in isolation, and the fact that Cloud computing allowed law enforcement to effectively search information contained in the home.[85]

The most recent United States Supreme Court case to address the issue of digital privacy was *Carpenter v. United States*.[86] The case challenged the application of the third-party search doctrine to cell-site location information (CSLI).[87] Prior to the opinion, state and federal courts remained divided on issues relating to the third-party search doctrine.[88] *United States v. Davis* exemplifies this split. A majority of the *en banc* Eleventh Circuit held that the Supreme Court's decisions in *Smith* and *Miller* were controlling and, thus, the defendant had no reasonable expectation of privacy in his cell-site location information.[89] However, two separate lower court concurrences called on the Supreme Court to clarify the scope of *Smith* and *Miller*. One concurrence written by Judge Rosenbaum was particularly compelling:

> In our time, unless a person is willing to live 'off the grid' it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life. And the thought that the government should be able to access such information without the basic protection that a warrant offers is nothing less than chilling . . . .[90]

Chief Justice John Roberts delivered the Supreme Court's opinion in *Carpenter* on June 22, 2018.[91] In the case, the Assistant United States Attorney investigating a string of robberies requested a court order to provide 152 days' worth of Carpenter's historical cell-site location data under the Stored Communications Act, 18 U.S.C. § 2703(d).[92] Under the Stored Communications Act, an order may be issued when the government "offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an

---

85 *Id*. at 2488–92.

86 *Carpenter v. United States*, 585 S. Ct. 2206 (2018).

87 Petition for Writ of Certiorari, *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017) (No. 16-402) http://www.scotusblog.com/wp-content/uploads/2016/10/16-402-cert-petition.pdf.

88 *Id*.

89 *Id.* at 12.

90 *Id*.

91 *Carpenter v. United States*, 585 S. Ct. 2211 (2018).

92 *Id*. at 2212.

ongoing criminal investigation."[93] The "reasonable grounds" standard requires significantly less than probable cause.[94] Federal magistrate judges issued two court orders directing MetroPCS and Sprint to disclose Carpenter's location information.[95]

Carpenter was charged with six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence.[96] Prior to trial, Carpenter moved to suppress the cell-site data provided by the wireless carriers on the basis that the government's failure to obtain a warrant prior to accessing his data violated his Fourth Amendment rights.[97] The district court denied the motion, the government relied on the location information at trial, and Carpenter was convicted.[98] The Court of Appeals for the Sixth Circuit affirmed, and the United States Supreme Court granted certiorari.[99]

The Supreme Court held in *Carpenter* that obtaining CSLI was a search under the Fourth Amendment and required a warrant in order to be valid.[100] The Court began its analysis by reaffirming that individuals have a reasonable expectation of privacy in the whole of their physical movements.[101] Then, the Court addressed the third-party search doctrine, which had been the government's main argument for obtaining the information.[102] The Court distinguished in nature and scope the search that occurred in *Carpenter* from the foundational third-party search doctrine cases, stating that "there is a world of difference between the limited types of person information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected [today] by wireless carriers."[103]

---

93 *Id*. (quoting 18 U.S.C. §2703(d) (2019)).

94 *Id*. at 2221 ("The Government acquired the cell-site records pursuant to a court order issued under the Stored Communications Act, which required the Government to show 'reasonable grounds' for believing that the records were 'relevant and material to an ongoing investigation.' That showing falls well short of the probable cause required for a warrant.") (quoting 18 U.S.C. §2703(d) (2019)).

95 *Id*. at 2212.

96 *Id*.

97 *Id*.

98 *Id*. at 2212–13.

99 *Id*.

100 *Id*. at 2221.

101 *Id*. at 2219.

102 *Id*.

103 *Id*. at 2217–19 ("Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whoever the suspect [of a crime] turns out to be, he has effectively been tailed every moment of every day . . . and the police may—in the Government's view—call upon the results of that surveillance without regard to the

Next, the Court distinguished the voluntary consent as being of a different kind than the foundational third-party search doctrine cases.[104] The Court stated that "carrying [a cell phone] is indispensable to participation in modern society[,]" and a user cannot meaningfully assume the risk of volunteering information to a third party because "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[105] As a result, the government should have been required to obtain a warrant prior to gaining access to Carpenter's cell-site location information.[106] However, the Court made explicitly clear that its decision in this case was "a narrow one[]" that did not "disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques . . . ."[107]

Thus, the Supreme Court has twice ruled to protect digital information derived from cell phones by requiring a warrant be obtained prior to gaining access to the user's information.[108] However, the Supreme Court has not yet ruled on whether a warrant would be required to access other types of digital information such as recordings from smart devices. Because the decision in *Carpenter* was a narrow one, the Court has left open the question of how much, if any, digital information from "always on" in-home technology would be subject to search by law enforcement and whether a warrant would be required to obtain access to this information.

IV. SUGGESTED SOLUTIONS

This Note argues that a warrant should be required when the government attempts to search recordings made by "always on" in-home technology. This solution is the most complete because it strikes an appropriate balance between governmental interests in enforcing the law and individual privacy interests: law enforcement officials can obtain sensitive digital information so long as they obtain a warrant before doing so.

Notably, this solution comes at the cost of making it more difficult for the police to solve crimes by preventing them from acquiring valuable evidence in criminal investigations. This begs the question: Should we

---

constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.").

104 *Id*. at 2220.

105 *Id*.

106 *Id*. at 2220–21.

107 *Id*. at 2220.

108 *Id*. at 2221; *Riley v. California*, 134 S. Ct. 2473, 2495 (2014).

make it more difficult for the government to obtain access to our most private information in order to solve crimes by requiring a warrant be issued before doing so?

The Supreme Court grappled with a similar question when it determined whether to apply the exclusionary rule to the states in *Mapp v. Ohio*.[109] Applying the exclusionary rule to the states would undoubtedly let guilty people walk free by excluding incriminating evidence from criminal trials because it was obtained by the police illegally.[110] After deciding that the exclusionary rule should be applied to the states, Justice Clark wrote for the majority in *Mapp* that, "[t]he criminal goes free, if he must, but it is the law that sets him free."[111] In *United States v. Leon*, the Court again confronted the exclusionary rule issue and attempted to balance governmental interests against the individual privacy protections engrained in the Fourth Amendment.[112] In ardent dissent, Justice Brennan wrote the following:

> While the machinery of law enforcement and indeed the nature of crime itself have changed dramatically since the Fourth Amendment became part of the Nation's fundamental law in 1791, what the Framers understood then remains true today—that the task of combating crime and convicting the guilty will in every era seem of such critical and pressing concern that we may be lured by the temptations of expediency into forsaking our commitment to protecting individual liberty and privacy. It was for that very reason that the Framers of the Bill of Rights insisted that law enforcement efforts be permanently and unambiguously restricted in order to preserve personal freedoms. In the constitutional scheme they ordained the sometimes unpopular task of ensuring that the government's enforcement efforts remain within the strict boundaries fixed by the Fourth Amendment . . . .[113]

Thus, while it is true that the solutions suggested in this Note will hinder law enforcement officers from solving crimes, as Justice Brennan observed, the Fourth Amendment demands protection of individual liberty against arbitrary government intrusion. To be clear, this Note does not suggest that the government should not be able to obtain access to any

---

109 *Mapp v. Ohio*, 367 U.S. 643, 646 (1961).
110 *Id.*
111 *Id.* at 659.
112 *United States v. Leon*, 468 U.S. 897, 900 (1984).
113 *Id.* at 929–30 (Brennan, J., dissenting).

digital information to aid in criminal investigations—just that it seek a warrant before doing so.

A. Why a Warrant Should be Required for Data from "Always On" In-Home Technology

In analyzing future cases, the Supreme Court would do well to extend the precedent set by *Riley* and *Carpenter* to data derived from "always on" in-home technology. The Court should find that the information derived from "always on" in-home technology is akin to that in *Carpenter* and is sensitive in nature and broader in scope than the information collected in *Smith* and *Miller*. Furthermore, the Court should find that "always on" in-home technology is akin to the CSLI collected in *Carpenter* because there is no meaningful consent for the collection of data from devices that are "always on."

The Supreme Court in *Carpenter* first distinguished the nature and scope of the information derived from *Smith* and *Miller* as being more limited in nature than that of CSLI.[114]

> The Government's position fails to contend with the seismic shift[] in digital technology [have] made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years . . . Unlike the nosy neighbor who keeps an eye on comings and goings, [Sprint Corporation and its competitors] are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronical of location information casually collected by wireless carriers today.[115]

The Court pointed out that the pen register in *Smith* had limited capabilities to reveal identifying information and the checks in *Miller* were negotiable instruments to be used in commercial transactions, not confidential communications.[116] The Court in *Riley* also addressed the sensitive nature of information derived from a cell phone and distinguished it in several important ways from information derived from other physical objects: A cell phone collects in one place many types of information that reveal much more in combination than in isolation; a cell

---

114 *Carpenter v. United States*, 585 S. Ct. 2206, 2219 (2018).
115 *Id*.
116 *Id*.

phone's capacity allows even one type of information to reconstruct the sum of an individual's private life; the data on the phone dates back to the phone's purchase or even earlier; and finally, a cell phone allows an individual to store in a portable location a great number of records that would not be accessible in a physical format.[117]

Like in *Riley* and *Carpenter*, information derived from "always on" in-home technology can be stored by Amazon or its competitors for years with infallible memory—smart device company servers also have immense storage capabilities, and it is common for recordings taken from "always on" devices to be stored for between six months to two years.[118] Also like cell phones, the aggregate of these recordings has the potential to reveal much more together than in isolation about an individual's private life and accessing aggregated recordings from a device from inside the home could, without a doubt, reveal an individual's religious, political, or sexual habits more than any one recording could in isolation.[119] For example, an Amazon Echo Dot that is located near a television would undoubtedly reveal snippets of any television program playing in the background during the user query, which could reveal information about the person's religious, political, or sexual habits.

"Always on" technology allows law enforcement officers to access digital recordings that were produced *inside a home*. Under normal circumstances, law enforcement officers would not be allowed to enter the home without a warrant unless one of the well-defined exceptions to the warrant requirement applied.[120] Law enforcement officers would certainly not be allowed to plant a recording device inside a home without a warrant.[121] But under the third-party search doctrine today, simply because the recordings from "always on" in-home devices were released to a third party, the government is effectively able to do indirectly what it could not do directly: Access recordings of consumers in their most intimate spaces without a warrant. Allowing the third-party search doctrine to swallow privacy protection in the home goes against the holdings in *Riley*, in *Carpenter*, and in Justice Scalia's majority opinion in *Kyllo* where he emphasized that "[i]n the home, our cases show, *all* details are intimate

---

117 *Riley v. California*, 134 S. Ct. 2473, 2489–90 (2014).

118 Tim Moynihan, *Alexa and Google Home Record What You Say. But What Happens to that Data?*, WIRED (Dec. 5, 2016), https://www.wired.com/2016/12/alexa-and-google-record-your-voice/.

119 McLaughlin, *supra* note 4. This problem is further exacerbated when more than one device is at issue. For example, as noted above James Bates had both an Amazon Echo Dot and a smart water device.

120 *Payton v. New York*, 445 U.S. 573, 576 (1980).

121 *Silverman v. United States*, 365 U.S. 505, 510–11 (1961).

details[.]"[122] Unlike the limited nature of the information in *Smith* and *Miller*, the fact that these recordings were made *inside a home* makes the likelihood that they contain sensitive information much greater and the need to protect this information much more significant.

The Court in *Carpenter* also distinguished the information derived from a cell phone on the basis that there is no meaningful consent to disclose the information to a third party as there was in *Smith* and *Miller*.[123] A cell phone automatically generates CSLI when it is powered on without any affirmative act on the part of the user, and there is no way to escape it doing so other than to remain off the grid.[124] As a result, the user does not in any meaningful sense volunteer this information to a third party and, thus, does not assume the risk of turning over the information to law enforcement.[125]

Information derived from "always on" in-home technology is also not volunteered to a third party in any meaningful sense. When one buys or installs a smart speaker or other "always on" in-home device, there is no warning label that indicates that the device may be recording you or turned over to law enforcement.[126] While it is true that cell phones are much more prevalent, a significant number of people own "always on" smart devices and use them within their homes.[127] These individuals do not suspect that these devices will be recording them in their most intimate spaces, saving those recordings on company servers, or sharing them with third party affiliates.[128] As a result, the Supreme Court should extend the holdings in *Riley* and in *Carpenter* to protect information derived from "always on" devices used inside a home and find that a warrant is required before this information is obtained by law enforcement.

---

122 *Kyllo v. United States*, 533 U.S. 27, 28 (2001).
123 *Carpenter v. United States*, 585 S. Ct. 2206, 2220 (2018).
124 *Id*. at 2219.
125 *Id*.
126 *See* Letter from Marc Rotenberg et al., *supra* note 17, at 4–5.
127 Perez, *supra* note 8.
128 Letter from Marc Rotenberg et al., *supra* note 17, at 4–5.

V. CONCLUSION

Under current Fourth Amendment jurisprudence, recordings from "always on" technology made inside a home are not protected from prying government eyes under the third-party search doctrine. A warrant should be required to obtain recordings from "always on" in-home devices. The year 1984 came and went without turning into Orwell's government surveillance nightmare. Today, no one should have to fear that recordings from their most intimate spaces can be provided to the government without their consent—or a warrant—because of the third-party search doctrine. No person should have to be afraid to speak candidly in his or her home for fear that "Big Brother is watching."