Stanford Law Review

Volume 72 February 2020

NOTE

Searching the Smart Home

Gabriel Bronshteyn*

Abstract. Upon the ratification of the Fourth Amendment in 1792, the privacy of the home gained constitutional stature. Courts have zealously guarded the home from warrantless invasion by the government ever since. Now, a flood of consumer-adopted technologies that promise convenience and companionship threatens the inviolability of the home in Fourth Amendment jurisprudence.

This Note explores the technical, constitutional, and theoretical privacy concerns raised by widespread adoption of "smart home" technology. After discerning a novel conceptual framework for assessing the Fourth Amendment's shifting contours in response to technological advances and assessing intersecting lines of applicable Fourth Amendment doctrine, the Note contends that data generated from within the home is worthy of constitutional protection. The Note concludes by suggesting that, rather than spelling the end of privacy in the home, smart home technology magnifies the "privacy as refuge" offered by the modern home.

* J.D. Candidate, Stanford Law School, 2020. I extend my deepest gratitude to David Sklansky for his guidance and profound insights. Many thanks as well to the editors of the *Stanford Law Review*—Tom Westphal, Nitisha Baronia, Justin Tzeng, Elisa Wulfsberg, and Nathan Lange, among others—for their invaluable editing and tireless work in bringing this piece to publication.

Table of Contents

Introduction

The Fourth Amendment protects houses from unreasonable searches.[1] For centuries, the U.S. Supreme Court has ardently enforced this historically rooted textual prohibition. Indeed, the image of the constable rummaging through private homes without permission or a warrant was the precise evil against which the Fourth Amendment's protections were drafted. But even as police replaced constables and Fourth Amendment cases became trickier, the Court remained steadfast, extending Fourth Amendment protection even to heat waves emanating from within homes[2] and smells perceptible to dogs on doorsteps.[3] In an exceptionally fact-bound area of constitutional law, the Supreme Court has drawn a "firm line" at the entrance of the home.[4]

But the home is starting to look different. The doors remain locked, but are now armed with cameras, microphones, and fingerprint scanners. The floors are still clean, but are now mopped by autonomous vacuums that develop internal blueprints of the home by continuously filming its interior. Sounds of conversation and laughter continue to echo through the halls, but the jokes and intimate confessions may now be shared between the residents and their smart home assistants. Each such innovation imports convenience or companionship into the home along with an array of sensors that export the data out to third-party servers.

Law enforcement and intelligence agencies have already begun taking notice of the vast quantities of profoundly intimate data being generated from within the "smart home." As smart home adoption and law enforcement interest in its surveillance value grow, smart home residents will increasingly look to the courts for constitutional privacy protection. After all, statutory protections may be inadequate. If the Stored Communications Act (SCA) even covers this data—and commentators suggest it may not[5]—the SCA imposes a substantially lower threshold for compelling data disclosure than the Fourth Amendment's probable cause standard, and allows voluntary disclosure by the electronic device manufacturers under some circumstances.[6] Fourth Amendment protection, on the other hand, would subject searches of smart

1. U.S. CONST. amend. IV.

2. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001).

3. *See* Florida v. Jardines, 569 U.S. 1, 11-12 (2013).

4. Payton v. New York, 445 U.S. 573, 590 (1980).

5. *See, e.g.*, Donald L. Crowell III, Note, *The Privacy of "Things": How the Stored Communications Act Has Been Outsmarted by Smart Technology*, 70 FED. COMM. L.J. 211, 227-28 (2018); Seth Weintraub, Comment, *Hey Alexa: Was It the Butler, in the Foyer, with the Candlestick? Understanding Amazon's Echo and Whether the Government Can Retrieve Its Data*, 7 AM. U. BUS. L. REV. 155, 172-75 (2018).

6. *See* 18 U.S.C. §§ 2702(b)(3)-(7), 2703(b)-(c) (2018).

home data to a warrant requirement. And as this Note contends, the Fourth Amendment's protections may apply even for data stored by smart home device manufacturers.

To be sure, smart home residents may face an uphill battle even under the Fourth Amendment. The smart home places traditional Fourth Amendment protections for the home on a collision course with the third-party doctrine, which generally excludes information willfully disclosed to a third party from the Fourth Amendment's coverage. The government may therefore argue that disclosures by smart home device manufacturers made voluntarily or pursuant to SCA requests are not Fourth Amendment searches at all. And perhaps the canonical level of privacy afforded to the home should be rethought in light of the deluge of sensors, microphones, and cameras being introduced into its walls.

This Note contends that such data is nonetheless worthy of Fourth Amendment protection. Part I examines the mass adoption of smart home technology and its potential as a law enforcement and surveillance apparatus. Part II formulates a conceptual framework for assessing the Fourth Amendment's evolution in response to technologies that reshape the dynamic between people and police. This framework reveals that the factors driving the Fourth Amendment's shifting doctrinal contours compel extending Fourth Amendment protection to smart home data. Part III surveys the intersecting lines of Fourth Amendment doctrines implicated by the smart home—namely, the primacy of the Fourth Amendment home, the digital privacy framework developed by the Supreme Court in *Riley v. California*,[7] and the third-party doctrine after *Carpenter v. United States*.[8] The Part first concludes that these doctrines support a finding that smart homes are covered by the Fourth Amendment. It goes on to suggest that the smart home exposes the need to disavow aspects of the third-party doctrine to bring the Fourth Amendment into the modern era. Finally, Part IV argues that the smart home requires a reimagination of privacy in the home, from "informational privacy" to a notion of privacy that understands the home as a "refuge." More sensors may indeed mean the end of informational privacy in the home. But even as it causes individuals' control over data flows to evaporate, the smart home could invigorate another dimension of privacy—"privacy as a refuge"—by augmenting the intimacy of people's interactions with their homes.[9]

7. 134 S. Ct. 2473 (2014).

8. 138 S. Ct. 2206 (2018).

9. Though the implications of the smart home for policing, the Fourth Amendment, and privacy have been lightly explored in the literature, this Note breaks new ground by highlighting law enforcement uses of smart home data; situating searches of smart home data within a novel conceptual framework for the Supreme Court's approach to the Fourth Amendment in light of evolving technology; evaluating the applicability of
footnote continued on next page

I. The Specter of Self-Surveillance in the Modern Home

Probing the legal and privacy implications of the modern home requires an appreciation of the technological revolution sweeping across the world and through our homes. "Smart home" technology generates an unprecedented volume of intimate data from within our homes, painting a vivid portrait of the "privacies of life."[10] The privacy concerns raised by adoption of such technology are neither hypothetical nor far off. The smart home is a problem of both the present and future, poised to become ubiquitous in modern society and already adopted by millions of American consumers.[11] This Part provides an overview of the growing web of sensors populating American homes, explaining what these devices are and the intimate data they generate. Most critically, this Part explores the smart home's potential as a surveillance or investigative apparatus for law enforcement.

A. Sensing Our Behavior: "Internet of Things" Devices

An exceptional share of data being generated from within homes originates from "smart devices"—internet-enabled versions of ordinary objects

---

the third-party doctrine to smart home data in light of *Carpenter*; and demonstrating how smart home technology augments the refuge offered by the modern home.

Other scholarship takes a different approach to the subject. *See generally, e.g.*, Stefan Ducich, *These Walls* Can *Talk! Securing Digital Privacy in the Smart Home Under the Fourth Amendment*, 16 DUKE L. & TECH. REV. 278 (2018) (contending that an exclusion framework should replace the trespass test to better accommodate the privacy threat posed by smart homes); Allegra Bianchini, Note, *Always On, Always Listening: Navigating Fourth Amendment Rights in a Smart Home*, 86 GEO. WASH. L. REV.: ARGUENDO 1 (2018) (arguing that Congress should amend the Electronic Communications Privacy Act of 1986 to cover "noncommunicative" data so as to protect smart home data); Christopher B. Burkett, Note, *"I Call Alexa to the Stand": The Privacy Implications of Anthropomorphizing Virtual Assistants Accompanying Smart-Home Technology*, 20 VAND. J. ENT. & TECH. L. 1181 (2018) (arguing that virtual assistants should be considered "persons" and extended a new privilege); Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924 (2017) (suggesting that the smart home reveals the limits of the third-party doctrine); Anne Pfeifle, Comment, *Alexa, What Should We Do About Privacy? Protecting Privacy for Users of Voice-Activated Devices*, 93 WASH. L. REV. 421 (2018) (arguing for privacy protections to be engineered into smart home devices); Weintraub, *supra* note 5 (evaluating the applicability of federal wiretap laws to Amazon Echo voice recordings and suggesting expanded statutory protections); Eric Boughman et al., *"Alexa, Do You Have Rights?" Legal Issues Posed by Voice-Controlled Devices and the Data They Create*, BUS. L. TODAY (July 15, 2017), https://perma.cc/KLR5-GFY2 (providing an overview of the legal issues raised by the adoption of smart home technology).

10. *See* Boyd v. United States, 116 U.S. 616, 630 (1886).

11. *See infra* text accompanying notes 14-17.

equipped with sensors and digital communication capabilities.[12] These devices make up what is known as the "Internet of Things"—"a wave of tech innovations that could turn once-mundane appliances like ovens, thermostats, microwaves, fridges and garage-door openers into a network of devices that communicate with each other."[13]

Consumer adoption of smart devices is widespread. Consumers are "the largest user[s] of connected things with 5.2 billion units in 2017, which represents 63 percent of the overall number of applications in use."[14] The home in particular is a central battleground for companies selling smart device technology to consumers.[15] In a 2018 study, 59% of American adults surveyed were interested in using a smart home device.[16] Consumer research forecasts that 26.7 million American homes—or 20% of households—will include smart devices (not including smart speakers), such as refrigerators, vacuums, and door locks, by 2022.[17]

Convenience is a significant motivation behind the mass adoption of smart home devices,[18] but the market goes far beyond staple devices transformed for convenience. As elaborated below, devices that offer entertainment, medical support, and even companionship are the next frontier in smart home innovation.[19] The cumulative effect is that modern homes are increasingly replete with sensors embedded in myriad objects. Each such device captures data about the consumer, creating a rich tapestry of information across an expanding number of devices deployed within people's homes.

---

12. *See* Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 554 n.24 (2017) ("No single agreed-upon definition exists about the term 'smart device.' Used here, the term signifies a generic device that has digital communication capabilities with other sensors.").

13. Caleb Garling, *Google Enters Homes with Purchase of Nest*, S.F. CHRON., Jan. 14, 2014, at DC6. The term "Internet of Things" was likely coined by Kevin Ashton in 1999 in reference to burgeoning radio-frequency identification technology. *See* Kevin Ashton, *That "Internet of Things" Thing*, RFID J. (June 22, 2009), https://perma.cc/22BE-MR8W.

14. Press Release, Gartner, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016 (Feb. 7, 2017) (citation omitted), https://perma.cc/F2SH-W3VW.

15. *See* Janet Morrissey, *The Race to Create the Coolest Smart Home Devices Is Hotter than Ever*, N.Y. TIMES (Jan. 15, 2019), https://perma.cc/F8FS-37GF (describing the rise of smart home devices).

16. FRANK E. GILLETT ET AL., FORRESTER RES., SMART HOMES ADVANCE TOWARD SUBSCRIPTION LIVING: HOW THE SUBSCRIPTION ECONOMY WILL DRIVE SMART HOME ADOPTION 3, 5 fig.1 (2018).

17. *Id.* at 3, 6 fig.2.

18. Morrissey, *supra* note 15.

19. *See infra* text accompanying notes 25-29, 308-15.

Our tour through the modern home—equipped with today's Internet of Things devices—begins at the door, where many Americans have installed smart locks and doorbells that capture and store data, including video and sound, about each person who enters or approaches the home.[20] The video can be accessed remotely, through a mobile phone or computer.[21] Some such locks also use the resident's biometric data, such as a fingerprint, to facilitate easy access to the home.[22] Inside, the floor glistens, recently vacuumed and mopped by an autonomous smart vacuum that traverses the home in the resident's absence, guided by a map of the home it has created by using a camera to survey its interior.[23] Behind the door hangs a smart umbrella that reminds anyone heading out the door when the rain is coming and offers location tracking via Bluetooth technology.[24] "'Magic' pill bottles" have also become a reality, flashing blue in the entryway to remind the resident to take her medicine.[25] "Sensors in the bottle detect when the cap is twisted," determine how much medicine remains in the bottle, and relay data about each patient's medication regimen to a centralized system.[26] In the living room, the Smart TV flickers on, capturing information about the occupant's viewing habits[27]—including whether they watch Fox News or CNN[28]—but also, less obviously, recording the conversations in the living room.[29] The security system has ears, too—

20. *See* Jon Chase, *The Best Smart Locks*, WIRECUTTER, https://perma.cc/8F7T-JPRB (last updated Dec. 13, 2019); Steven John, *The Ring Video Doorbell Lets You Watch Over Your Home, Even when You're a Thousand Miles Away—Here's How It Works*, BUS. INSIDER (Feb. 12, 2019, 11:30 AM), https://perma.cc/45X9-W573.

21. John, *supra* note 20.

22. Chase, *supra* note 20.

23. *See* Maggie Astor, *Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared*, N.Y. TIMES (July 25, 2017), https://perma.cc/CK3V-GZXQ; Liam McCabe, *The Best Robot Vacuums*, WIRECUTTER, https://perma.cc/XTZ7-B9T8 (last updated Dec. 3, 2019).

24. *See* Press Release, Weatherman, The Unforgettable Umbrella Has Arrived—Weatherman (Nov. 16, 2017), https://perma.cc/BY2P-PDRZ; *see also* DAVID ROSE, ENCHANTED OBJECTS: DESIGN, HUMAN DESIRE, AND THE INTERNET OF THINGS 109-10 (2014) (describing an earlier version of a smart umbrella).

25. *See* ROSE, *supra* note 24, at 9; Lauren Silverman, *"Smart" Pill Bottles Aren't Always Enough to Help the Medicine Go Down*, NPR: SHOTS (updated Aug. 23, 2017), https://perma.cc/E5BA-BRKD.

26. Silverman, *supra* note 25.

27. *See* Geoffrey A. Fowler, *You Watch TV. Your TV Watches Back.*, WASH. POST (Sept. 18, 2019, 5:00 AM PDT), https://perma.cc/V3WC-7C6G.

28. A person's choice of news station is a powerful predictor of political preferences. *See, e.g.*, Joel Rose, *Poll: Where You Watch TV News Predicts Your Feelings on Immigration*, NPR (July 16, 2018, 5:09 AM ET), https://perma.cc/3XFV-36HT.

29. *E.g.*, Chris Matyszczyk, *Samsung's Warning: Our Smart TVs Record Your Living Room Chatter*, CNET (Feb. 8, 2015, 2:10 PM PST), https://perma.cc/T9GU-V252.

Google just didn't mention them.[30] In the kitchen, the smart refrigerator displays each family member's schedule.[31] Inside, a camera monitors the resident's available food and ingredients for remote viewing.[32] Conveniently, the fridge is a portal to nearly every other gadget in the smart home, combining the control of and data generated by each device into a handy, centralized platform.[33] It can even mirror the contents of the resident's smart phone for easy access.[34] The house is littered with similar gadgets: ordinary objects equipped with sensors and wireless connectivity, capturing data about the occupant in the name of greater functionality and convenience. In case we care to revisit this tour through the home later, the smart cameras arranged discreetly throughout the home have been following and recording us, using 3D sensors and artificial intelligence to monitor our behavior with such precision that asking them "why is the vase broken?" would yield video evidence of the precise moment the dog knocked it over.[35]

That is the smart home of today—and only a brief look at the array of devices available for purchase. The smart home of tomorrow will feature more gadgets that capture increasingly intimate insights into our private home lives. With each passing day, "[t]ech giants and start-ups alike are rolling out innovative [smart] devices at a breathtaking pace—the quirkier and more eye-catching the better."[36] "Phillips [sic], GE, Amazon, Apple, Google, Microsoft, Tesla, Samsung, and Nike are all working on products with embedded [Internet of Things] functionality . . . ."[37] And the technology will progressively be integrated into new homes as a standard feature rather than adopted on an opt-in, piecemeal basis by the consumer.[38] Health-driven applications of networked sensor technology in particular will radically transform the sort of information people will generate from within their home. An MIT professor is developing a box that monitors the electromagnetic field surrounding each occupant of an entire home, tracking physiological signals about "breathing,

30. *E.g.*, Taylor Telford, *Google Failed to Notify Customers It Put Microphones in Nest Security Systems*, WASH. POST (Feb. 20, 2019, 11:41 AM EST), https://perma.cc/2CWE-2N4H.

31. *See, e.g.*, Ry Crist, *Here's What's Next for Samsung's Family Hub Smart Fridge*, CNET (Jan. 7, 2018, 2:00 PM PST), https://perma.cc/TB52-65S7.

32. *Id.*

33. *Id.*

34. *Id.*

35. *E.g.*, Janet Morrissey, *In the Rush to Join the Smart Home Crowd, Buyers Should Beware*, N.Y. TIMES (Jan. 22, 2019), https://perma.cc/79BL-BDHP.

36. Morrissey, *supra* note 15.

37. MATTHEW G. OLSEN ET AL., DON'T PANIC. MAKING PROGRESS ON THE "GOING DARK" DEBATE 13 (2016), https://perma.cc/2W6T-C42X.

38. *See, e.g.*, R.A. Schuetz, *McGuyer Homebuilders Moves to Make All New Builds Smart Homes*, HOUS. CHRON. (Feb. 4, 2019), https://perma.cc/S9TN-UA27.

heart rate, sleep, gait, and more."[39] Another company hopes to place smart toilets in each home that "will be analyzing human waste in real time every day" to save customers a trip to the doctor.[40] In addition to endorsing waste-analyzing toilets, Deana McDonagh, a professor and design strategist, imagines the smart bathroom going further: "[I]n the shower, or while you're brushing your teeth, mats could weigh you and little cameras that you control could identify things like precancerous growths . . . ."[41]

The physical presence of these devices alone raises important technical and privacy considerations.[42] There are well-documented vulnerabilities common to many such devices that continue to be explored and documented by hackers and security organizations.[43] But the greater concern is that even the most secure devices tend to store the data generated from within the home in "the cloud," or on third-party servers.[44] To make the problem worse, different manufacturers' devices and cloud-based services often share data among themselves, increasing the number of parties with access to the web of information generated by smart devices within the home.[45] Even when there is no overt cross-functionality, apps that run on smartphones, smart home assistants, and other smart home technology platforms reportedly share private data collected by the applications—from heart rate, to interest in buying a home, to whether the user is ovulating—with larger technology companies like Facebook, Amazon, Apple, or Google.[46] Many of these apps share data with companies like Facebook whether or not the user is logged in via Facebook and without a way to opt out.[47] The way data is generated,

39. Rachel Metz, *Soon Your Doctor Will Be Able to Wirelessly Track Your Health—Even Through Walls*, MIT TECH. REV. (Sept. 12, 2018), https://perma.cc/7PEW-EKKH.

40. Stephen Shankland, *AI Toilets Will Scan Your Poop to Diagnose Your Ailments*, CNET (Nov. 12, 2018, 3:46 PM PST), https://perma.cc/BG7X-TA8T (quoting Sanjay Mehrotra, CEO, Micron Technology).

41. Lexi Pandell, *The Messy Future of Connected Bathrooms*, N.Y. MAG.: INTELLIGENCER (July 18, 2018), https://perma.cc/56R9-29ZT (quoting Deana McDonagh, Professor, University of Illinois).

42. *See generally* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805 (2016).

43. *See id.* at 819-22; Morrissey, *supra* note 35.

44. Ferguson, *supra* note 12, at 562 ("[M]ost data trails arising from the Internet of Things can also be obtained via the third party provider (usually the private company collecting the data) . . . .").

45. *See supra* text accompanying note 33.

46. For one example, see Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J. (Feb. 22, 2019, 11:07 AM ET), https://perma.cc/NS9M-5LR2. *See also* Astor, *supra* note 23 (describing how some Roombas collect mapping data of the home that the company iRobot "could share with Amazon, Apple, or Google").

47. *See* Schechner & Secada, *supra* note 46.

shared, and stored magnifies the privacy concerns associated with the mass adoption of smart home technology, making it increasingly difficult to track where massive volumes of intimate user data are ultimately stored and with whom they are shared.

B. Hearing Our Thoughts: Smart Home Assistants

Discussion of the smart home would be incomplete without reference to preeminent smart home assistants like Google Home and Amazon Echo (often referred to as "Alexa," the name of the humanoid voice that responds to user commands and questions[48]). Smart home assistants are small, interactive devices that, in response to a user's directive, can perform a wide range of tasks, including playing certain songs, checking the weather, telling jokes, and controlling the other smart devices installed throughout the home.[49] The Echo is known as an "always on, always listening" device because it works by listening for its "wake words," which prompt the device to record the user's voice.[50] The device sends the voice recording to a platform run on the company's servers (a practice called "server-side processing"), which interprets the voice recording, extracts a command, and directs the device to carry it out.[51]

Along with answering questions and turning on the lights, smart home assistants generate and collect data. When they work as a centralized hub through which users may control other devices, smart home assistants interact with the data generated throughout the home by the Internet of Things devices discussed in Part I.A.[52] More pressingly, these devices not only passively capture the words spoken by residents in the privacy of their home, but also affirmatively engage in interactions that prompt revelations that users might not have otherwise shared.[53]

The privacy implications are in some ways obvious. The concept of a device sitting in the home, always on and always listening, stoked fear, skepticism, and comparisons to *1984* when the Echo devices were first

48. Richard Baguley & Colin McDonald, *Appliance Science: Alexa, How Does Alexa Work? The Science of the Amazon Echo*, CNET (Aug. 4, 2016, 5:00 AM PDT), https://perma.cc/R6EQ-MF5Y.

49. *See id.*; *see also* Alina Bradford, *The Funniest Things to Ask Alexa*, DIGITAL TRENDS (Oct. 28, 2019, 2:12 PM PST), https://perma.cc/A6KN-258K.

50. *See* Baguley & McDonald, *supra* note 48.

51. *See id.*

52. *See* Daniel Wroclawski, *How to Use Alexa to Control Your Smart Home*, CONSUMER REP., https://perma.cc/62UB-2URT (last updated May 14, 2019).

53. *See infra* notes 59-62 and accompanying text.

announced by Amazon.[54] But people got over it. More than 100 million Alexa-equipped devices[55] and 52 million Google Home devices[56] have been sold globally as of early 2019. Of those Google Home devices, 43 million were installed in the United States.[57] And as the devices become more popular, the privacy concerns are amplified—not only because more conversations are captured, but also because the dynamic of human interaction with smart home assistants evolves with their increasing adoption and technological advancement.

Initially, people worried about the conversations smart home assistants might overhear.[58] But the greater privacy threat posed by such devices, and the more useful data for law enforcement, may be the conversations users have directly with their digital assistants. For research purposes, I purchased an Amazon Echo device, and was surprised at the fluidity with which it (or "she," as I've begun to reflexively call it/her) understands and responds to commands. The device engages in banter, intuitively digests complicated requests, and even has opinions.[59] More than 50% of user interactions are "nonutilitarian"—seeking entertainment or companionship instead of the comparatively simple functionality for which Alexa is designed.[60] It is no wonder, then, that in addition to asking Alexa to order an extra set of dryer sheets from Amazon, people have begun confiding in her in deeply personal ways, including sharing thoughts of suicide, experiences of abuse, and other private information.[61] As

54. *See, e.g.*, Alex Fitzpatrick, *Your Gadgets May Soon Be Spying on Your Conversations*, TIME (Nov. 11, 2014), https://perma.cc/25DV-3PCH ("[A]lways-listening devices like Echo . . . come with a certain creep factor. After the Snowden leaks, it's a big ask of Amazon or any other company for us to put Internet-connected, always-listening microphone [sic] in our homes. The *1984* comparisons write themselves, and aren't totally without precedent.").

55. Abrar Al-Heeti, *Amazon Has Sold More than 100 Million Alexa Devices*, CNET (Jan. 4, 2019, 3:51 PM PST), https://perma.cc/MW3B-8Y74.

56. Jillian D'Onfro, *Google's Small Hardware Business Is Shaping Up, Could Book $20 Billion in Sales by 2021, RBC Says*, CNBC (updated Dec. 21, 2018, 12:05 PM EST), https://perma.cc/PT4Q-VXKE.

57. *Id.*

58. *See* Fitzpatrick, *supra* note 54.

59. For example, fans of Lebron James will be disappointed to learn that when I asked Alexa, "who is the greatest basketball player of all time," it replied, "I've got to say Jordan is the G.O.A.T." before rattling off a number of impressive statistics about Michael Jordan's playing career.

60. Laura Stevens, *"Alexa, Can You Prevent Suicide?": How Amazon Trains Its AI to Handle the Most Personal Questions Imaginable*, WALL ST. J. (Oct. 23, 2017, 8:38 AM ET), https://perma.cc/WCV3-SZ2K.

61. *Id.*

Alexa gets smarter, more empathetic, and more human,[62] we should expect her to learn increasingly intimate details about people's inner lives—thoughts, feelings, and memories previously inaccessible to law enforcement except by interrogation, wiretapping, or undercover agents.

C. The Smart Home as a Police Tool

Though some smart devices raise privacy concerns more directly than others, the cumulative effect of filling homes with interconnected sensors can transform even trivial data generated by ostensibly innocuous devices into a mosaic of intimate information from which law enforcement can make profound inferences. Andrew Ferguson has described this self-imposed surveillance as "sensorveillance—the ever-increasing ability for surveillance technologies to track individuals through the data trails they leave behind."[63] The inferential power of combining information from different sources of data—termed the "mosaic effect"[64]—is a well-recognized consequence of smart device adoption.[65] Individual sensor data points may not be incriminating, but they "tend to combine in unexpected ways, giving rise to powerful inferences."[66] As Scott Peppet points out, "[s]ensor data capture incredibly rich nuance about who we are, how we behave, what our tastes are, and even our intentions. . . . [T]hese data are the grist for drawing revealing and often unexpected inferences about our habits, predilections, and personalities."[67] For a strange example, consider the smart refrigerator discussed earlier.[68] An inventory of a resident's fruits and vegetables sounds innocuous, but Samsung

62. *See* Laura Stevens, *"Alexa, Can You Be Empathetic, All-Knowing and Funny?,"* WALL ST. J. (Mar. 7, 2019, 10:04 AM ET), https://perma.cc/YS6D-JYHE ("In the future, a conversation with a digital assistant will be indistinguishable from one with a person . . . .").

63. Ferguson, *supra* note 12, at 551.

64. The "mosaic effect" phenomenon has been studied in the legal scholarship in other contexts, and partially adopted by the Supreme Court as a lens through which to view the privacy implications of modern technology. *See, e.g.*, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012); Note, *Data Mining, Dog Sniffs, and the Fourth Amendment*, 128 HARV. L. REV. 691, 692 (2014); *see also* Riley v. California, 134 S. Ct. 2473, 2489 (2014) (noting that "a cell phone collects in one place many distinct types of information . . . that reveal much more in combination than any isolated record"). See Part III.B below for an extended discussion of the mosaic theory of the Fourth Amendment in the context of the smart home.

65. *See, e.g.*, Ferguson, *supra* note 42, at 820; Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 90 (2014).

66. Peppet, *supra* note 65, at 120.

67. *Id.* at 90.

68. *See supra* text accompanying notes 31-34.

has already capitalized on the inferential power of that limited data in a surprising way, releasing a "Refrigerdating" app that matches people "with the help of the contents of the fridge, because that can tell you a lot about [one's] personality."[69]

The mosaic effect of smart home device adoption should raise even greater privacy concerns given the rise of algorithmic, data-driven policing, which provides law enforcement with the analytical tools to draw inferences by combining innocuous sources of data littered throughout people's homes.[70] Such tools use machine learning algorithms and statistical modeling techniques to extract inferences and patterns from data.[71] Governments can feed these algorithms personal data about potential or convicted criminals to produce a quantitative assessment of those individuals' likelihood of engaging in criminal behavior. For example, police departments can and do use predictive policing tools to assess risk and determine how to distribute their crime-fighting resources.[72] Data-driven policing programs, still in their infancy, are increasingly becoming adopted by police forces across the country.[73] No police department on record has used this technology to derive inferences from smart home devices so far, but expanding police reliance on machine learning and big data reveals the surveillance threat of the smart home.

Big data's contribution to policing is relatively new, but its role in intelligence is firmly established and widely known, thanks to revelations by

69. Erin Carson, *Samsung Tries to Turn Your Refrigerator into Tinder*, CNET (Feb. 5, 2019, 5:02 AM PST), https://perma.cc/JE3Q-VUQE (quoting a Samsung representative).

70. Data-driven predictive policing has also been the subject of extensive criticism on the grounds that it reinforces historical biases in the criminal justice system, an important issue outside the scope of this Note. For more, see, for example, ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 5-6 (2017) (describing the future of policing in the age of "big data" and evaluating the risks to freedom and privacy posed by new investigative and surveillance technologies); BERNARD E. HARCOURT, AGAINST PREDICTION: PROFILING, POLICING, AND PUNISHMENT IN AN ACTUARIAL AGE 2-6 (2007) (arguing for a "presumption against prediction," partially because of the distorting effects of actuarial methods in criminal investigation and sentencing (emphasis omitted)); Sonja B. Starr, *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, 66 STAN. L. REV. 803, 821-41 (2014) (arguing that evidence-based sentencing violates the Equal Protection Clause); and Karen Hao, *AI Is Sending People to Jail—and Getting It Wrong*, MIT TECH. REV. (Jan. 21, 2019), https://perma.cc/Z67P-5WFN (contending that populations "that have historically been disproportionately targeted by law enforcement—especially low-income and minority communities—are at risk of being slapped with high recidivism scores").

71. *See* Hao, *supra* note 70.

72. *Id.*

73. *See, e.g.*, Press Release, Office of the Mayor, City of Chicago, CPD Continues Expansion of Predictive Technology to Support Strategic Deployments, Reduce Crime (Mar. 4, 2018), https://perma.cc/K5EJ-A9G7.

Edward Snowden. Snowden was a 29-year-old National Security Agency (NSA) intelligence analyst who stole 1.7 million documents and uncovered PRISM, a surveillance program of startling breadth that procured and analyzed conversations between U.S. citizens from major technology companies.[74] Given the secrecy and scale of the NSA surveillance revealed by Snowden's leaks, it is unsurprising that intelligence agencies have already keyed in on smart home technology as a source of intelligence.[75] In 2016, James Clapper, the U.S. Director of National Intelligence, submitted testimony to the Senate signaling a desire to seize upon "new opportunities for our own intelligence collectors" created by innovations in information technology.[76] "In the future," he explained, "intelligence services might use the [Internet of Things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials."[77] The extent of other existing surveillance of smart home devices by the NSA or other intelligence agencies remains unknown.

Both predictive policing and NSA data collection are sufficiently abstract and large scale that consumers appear not to be fazed by the surveillance issues they raise. But law enforcement has also begun leveraging the data generated by smart home devices for more traditional investigative purposes.

On November 22, 2015, James Bates reportedly found Victor Collins dead in Bates's hot tub.[78] Suspicious that Bates's Echo device had been used to play music the night of Collins's death, the police seized the device and subsequently issued search warrants to Amazon seeking audio recordings and transcriptions of the forty-eight-hour period surrounding Collins's death.[79] Amazon contested the warrant on First Amendment grounds[80] but ultimately relented, providing the data to the Arkansas police after Bates consented.[81] A judge has ordered a search warrant on Amazon Echo device data without user consent, too. In November 2018, a New Hampshire judge ordered Amazon to turn over

74. Lexi Mealey, *We Still Need to Talk About Edward Snowden*, HARV. POL. REV. (Jan. 18, 2018), https://perma.cc/6VE9-8CBK.

75. *See* JAMES R. CLAPPER, DIR. OF NAT'L INTELLIGENCE, WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY 1 (2016), https://perma.cc/56M8-R4LN.

76. *Id.*

77. *Id.*

78. Zuzanna Sitek & Dillon Thomas, *Bentonville PD Says Man Strangled, Drowned Former Georgia Officer*, 5 NEWS ONLINE (updated Feb. 23, 2016, 10:43 PM), https://perma.cc/7K84-CRKQ.

79. *See* Affidavit for Search Warrant at 4-6, State v. Bates, No. CR-16-370-2 (Ark. Cir. Ct. Aug. 26, 2016).

80. Memorandum of Law in Support of Amazon's Motion to Quash Search Warrant at 9-15, *Bates*, No. CR-2016-370-2 (Ark. Cir. Ct. Feb. 17, 2017).

81. Stipulation & Consent Order at 1, *Bates*, No. CR-2016-370-2 (Ark. Cir. Ct. Mar. 6, 2017).

forty-eight hours of user recordings based on police suspicion that the device, sitting on the countertop, may have been listening during a double murder.[82]

Searches of Amazon Echo recordings are perhaps the most publicized examples of smart home devices serving law enforcement ends, but they are not the only ones. In June 2015, federal officers in San Diego applied for a search warrant for information from the Samsung Smart TV of Mikhail Feldman, a man formerly convicted of possessing child pornography.[83]

Another example showcases the inferential power of combining different sources of data from the smart home. Two days before Christmas Day in 2015, police arrived to a Hartford, Connecticut, home to find Connie Dabate dead and her husband Richard Dabate bleeding and tied to a chair.[84] Richard told police that a masked intruder had tortured him and killed his wife in front of him.[85] Finding little physical evidence, the police turned to data from the victim's step-counting Fitbit device, smart alarm system, and key fob, among other devices.[86] The data came together to reveal that Richard's account of the night was "an elaborately staged fiction."[87] Connie's Fitbit showed that she was moving around the house nearly an hour after Richard had said she died.[88] And the home's smart alarm system raised doubts about whether he had, as he claimed, left home that morning.[89] Richard, whose scheme unraveled because of data generated by his smart home, was ultimately charged with his wife's murder.[90] He pled not guilty,[91] which will offer prosecutors the opportunity to make their case to the jury using data from his smart home.

These stories are telling, but they reveal only a slice of the government's increasing reliance on smart home technology as an investigative tool. Most cases are not reported publicly the way the cases above were. According to a transparency report from Nest Labs, Google's smart home division that sells

82. 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, 4:28 AM PST), https://perma.cc/FEJ6-AJGA; *see also* Order on Motion to Search in Lieu of Search Warrant at 1-2, State v. Verrill, No. 219-2017-CR-072 (Strafford Cty., N.H. Super. Ct. Nov. 5, 2018).

83. Application for a Search Warrant, *In re* Search of Samsung Smart TV, No. 3:15-mj-01985 (S.D. Cal. June 29, 2015), ECF No. 1.

84. Justin Jouvenal, *Commit a Crime? Your Fitbit, Key Fob or Pacemaker Could Snitch on You.*, WASH. POST (Oct. 9, 2017), https://perma.cc/7P67-RN3Q.

85. *Id.*

86. *Id.*

87. *Id.*

88. *Id.*

89. *Id.*

90. *Id.*

91. *Id.*

smart alarms, doorbells, thermostats, and cameras,[92] governments have requested data from Nest on 300 occasions—affecting as many as 525 account holders—since 2015.[93] Amazon, which received 1,955 government subpoena orders overall in the first half of 2019, has declined to publish the number of such requests made for Echo device data.[94] Whatever the true number, it is clear that the government is becoming wise to the information-gathering potential of smart home devices.

II. A Conceptual Framework

Much of the Supreme Court's most difficult work in its evolving Fourth Amendment jurisprudence has been triggered by the advent of new technologies—including wiretaps,[95] pen registers,[96] Global Positioning System (GPS) monitoring devices,[97] thermal imagers,[98] and cell phones[99]—that offer law enforcement new opportunities for surveillance or investigation. Indeed, the modern test for what constitutes a Fourth Amendment "search" was developed by a Court wrestling with the implications of the "vital role that the public telephone ha[d] come to play in private communication."[100]

This Part offers a broad framing of the Court's approach to developing its Fourth Amendment jurisprudence in response to the advent of new technologies before applying that framework to the smart home. New technologies rarely fit neatly within the Court's existing tests. Applying old doctrinal rules to new technologies often produces unacceptable results that demand rethinking the doctrine and expanding the reach of the Fourth Amendment's protections.[101] Smart home devices in particular implicate a

92. *Nest & Google*, GOOGLE, https://perma.cc/Q7J7-PB5H (archived Nov. 3, 2019).

93. Thomas Brewster, *Smart Home Surveillance: Governments Tell Google's Nest to Hand Over Data 300 Times*, FORBES (Oct. 13, 2018, 8:31 AM), https://perma.cc/6STY-TTDD.

94. AMAZON, AMAZON INFORMATION REQUEST REPORT (2019), https://perma.cc/E2M7-E8SR.

95. *See* Katz v. United States, 389 U.S. 347, 348-49 (1967) (discussing surveillance of a public telephone booth using an "electronic listening" device).

96. *See* Smith v. Maryland, 442 U.S. 735, 736 (1979).

97. *See* United States v. Jones, 565 U.S. 400, 402 (2012); *see also* United States v. Karo, 468 U.S. 705, 707 (1984) (considering a more rudimentary "beeper" tracking device).

98. *See* Kyllo v. United States, 533 U.S. 27, 29 (2001).

99. *See* Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018); Riley v. California, 134 S. Ct. 2473, 2480 (2014).

100. *Katz*, 389 U.S. at 352.

101. Justice Alito illuminated this phenomenon in his concurrence in *United States v. Jones*. Responding to Justice Scalia's invocation of the eighteenth-century conception of the Fourth Amendment in a case about GPS monitoring of a vehicle, Justice Alito suggested that "it is almost impossible to think of late-18th-century situations that are analogous

footnote continued on next page

crisscrossing set of doctrinal frameworks and analogous cases.[102] Different cases employing diverse doctrinal tools can all be on point yet may be marshalled in favor of diverging conclusions about whether the Fourth Amendment reaches the data generated by smart home devices.[103] Therefore, a conceptual perspective on the Court's approach to the Fourth Amendment and technology is critical for assessing whether smart home data is entitled to Fourth Amendment protection.

A. The Fourth Amendment and Technology

Since the Supreme Court adopted the "reasonable expectation of privacy" test in *Katz v. United States*,[104] it has been forced to confront the difficult question of what constitutes a "reasonable" expectation of privacy in different contexts, prompted by innovations in the use and application of technology by consumers and law enforcement. In each case, the Court must grapple with the ways in which evolving technology has reshaped the dynamic between citizens and law enforcement, thereby changing citizens' privacy expectations. In some cases, the Fourth Amendment question arises from consumer adoption of new technology.[105] In others, law enforcement agencies' use of novel technology forces the Court to rethink its doctrine.[106] And still other cases are at the intersection of these categories because police have employed one technology in an innovative way to respond to consumer adoption of another

to what took place in this case." *Jones*, 565 U.S. at 420 (Alito, J., concurring in the judgment). He elaborated: "Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner?" *Id.*

102. *See infra* Part III.

103. *See infra* Part III.

104. Justice Harlan articulated the precise test in his concurrence. *See Katz*, 389 U.S. at 360-61 (Harlan, J., concurring).

105. For example, the Court had to grapple with the evolution of telecommunications technology from phone booths, *see Katz*, 389 U.S. 347 (evaluating whether wiretaps are Fourth Amendment searches), to personal electronic devices that *store* data, *see* Riley v. California, 134 S. Ct. 2473 (2014) (reexamining the search incident to arrest exception in the context of cell phones), to personal electronic devices that *generate* data, *see* Carpenter v. United States, 138 S. Ct. 2206 (2018) (assessing whether cell site location information is entitled to Fourth Amendment protection).

106. *See, e.g.*, *Jones*, 565 U.S. 400 (deciding the constitutionality of tracking a vehicle's location through the use of a GPS device installed on its undercarriage); Kyllo v. United States, 533 U.S. 27 (2001) (evaluating whether use of thermal imaging technology to detect heat emanating from within the home constitutes a Fourth Amendment search); United States v. Karo, 468 U.S. 705 (1984) (considering the constitutionality of warrantless tracking of an electronic "beeper" installed into a can of chemicals).

technology.[107] It is no wonder, given the boundless and unforeseeable ways in which technology can be used to either escape or enhance surveillance, that the Court has refused to adopt a single, straightforward approach to applying the nebulous "reasonable expectation of privacy" test.[108] As Justice O'Connor observed, the Court has "no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable."[109]

Fourth Amendment cases featuring new technologies are especially challenging both because they render reliance on precedent difficult and because they feature complex questions about shifting expectations of privacy. In these cases, the Court is often forced to adjust the Fourth Amendment's protections to reflect the realities of society's use of technology, and to safeguard people's use of that technology from what the Court perceives to be unacceptable surveillance or intrusion into people's private lives. Orin Kerr has described this phenomenon as "equilibrium-adjustment."[110] He explains that "[w]hen new tools and new practices threaten to expand or contract police power in a significant way, courts adjust the level of Fourth Amendment protection to try to restore the prior equilibrium."[111] Because new technology constantly upsets the balance of power between police and citizens, Fourth Amendment doctrine is "the product of hundreds of equilibrium-adjustments made over time."[112]

Kerr suggests that this process of equilibrium-adjustment maintains the balance between people and police present at "Year Zero—the original Fourth Amendment as understood at the time of the Framing."[113] In at least some opinions, the Court has embraced this historically oriented approach, framing its analysis as seeking to assure "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[114] But in many cases that feature evolution of Fourth Amendment doctrine in response

107. *See, e.g.*, *Carpenter*, 138 S. Ct. 2206 (examining police use of location data to track the owner of a cell phone); Smith v. Maryland, 442 U.S. 735 (1979) (addressing the constitutionality of warrantless use of a "pen register" to record numbers dialed by a telephone from within a suspect's home).

108. *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(a) (West 2019) ("The Supreme Court, quite understandably, has never managed to set out a comprehensive definition of the word 'searches' as it is used in the Fourth Amendment.").

109. O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (plurality opinion).

110. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

111. *Id.*

112. *Id.* at 481.

113. *Id.* at 531.

114. *E.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001).

to new technology, including *Katz*, the Court has made no effort to relate the privacy interests implicated by the technology to the level of privacy expected in 1791. And neither *Carpenter v. United States* nor *Kyllo v. United States*, both of which claimed to preserve the privacy that existed in the eighteenth century,[115] seriously engaged with eighteenth-century history or expectations of privacy.

Whether the Court is attempting to restore founding-era levels of privacy or simply employing the common-law method to ensure the law reflects the "felt necessities of the time,"[116] its evolving jurisprudence does reflect a corrective mechanism responsive to technologies that change the landscape of policing, privacy, and surveillance. In dealing with these technologies, the Court does more than toggle between higher and lower levels of Fourth Amendment protection depending on whether "changing technology or social practice makes evidence substantially easier" or harder "for the government to obtain."[117] The Court's analysis is more nuanced, taking different forms depending on whether the technology is consumer- or police-facing.

When the issue is prompted by a new law enforcement tool, the Court assesses the invasiveness of the government's use of the new technology. In *Kyllo*, the Court held that police use of thermal imaging technology constituted a Fourth Amendment search because it provided the government "information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area.'"[118] Similarly, in *United States v. Karo*, the Court held that the use of a beeper device to track people within their homes was a search because it generated information from "private residences[,] places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant."[119]

As I will show, when faced with the Fourth Amendment issues implicated by consumer adoption of a new technology, the Court tends to approach the impact on society's reasonable expectation of privacy from two discrete angles: the invasiveness of a potential search (or the intimacy of the information revealed by a search of the technology) and the role of the technology in modern life. Both factors contribute to the Court's understanding of the extent to which the technology "has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes."[120] A ubiquitous

115. *See* Carpenter v. United States, 138 S. Ct. 2206, 2213-14 (2018); *Kyllo*, 533 U.S. at 34.

116. OLIVER WENDELL HOLMES, JR., THE COMMON LAW 1 (Harvard Univ. Press 2009) (1881).

117. *See* Kerr, *supra* note 110, at 480.

118. *Kyllo*, 533 U.S. at 34 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

119. 468 U.S. 705, 714-15 (1984).

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

technology with minimal privacy implications is unlikely to get the Court's attention. And a technology with profound privacy implications but extremely limited adoption, and therefore limited implications for government surveillance, is similarly unlikely to lead the Court to adjust its doctrine.

In *Katz*, the Court was faced with the question whether recording a phone call by surreptitiously placing a recording device on the outside of a phone booth constituted a search under the Fourth Amendment.[121] Under the then-prevailing trespass test from *Olmstead v. United States*, physical penetration akin to a trespass of a constitutionally protected space was necessary to consider police action a search.[122] In *Olmstead*, the Court held that eavesdropping on private conversations did not implicate the Fourth Amendment because "[t]here was no entry of the houses or offices of the defendants."[123] But the *Katz* Court reached the opposite conclusion, holding that listening to Mr. Katz's phone call was a search under the Fourth Amendment because it "violated the privacy upon which he justifiably relied."[124] In the words of Justice Harlan, who articulated the modern test for Fourth Amendment searches,[125] electronic intrusion into a phone booth violated Mr. Katz's "constitutionally protected reasonable expectation of privacy."[126]

The Court's dramatic course correction, expressed in a brief twelve-page opinion, was prompted by its reckoning with the consequences of maintaining the common law trespass test in the modern age of the telephone. The Court explored the issue from two angles. First, the Court evaluated the substantive privacy interests at stake, writing: "One who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[127] Second, the Court famously recognized that adopting a narrower construction of the Fourth Amendment—one that did not protect the privacy of phone booth users—would "ignore the vital role that the

121. Katz v. United States, 389 U.S. 347, 348-49 (1967).

122. *See* 277 U.S. 438, 457, 466, 468 (1928), *overruled by Katz*, 389 U.S. 347.

123. *Id.* at 464.

124. *Katz*, 389 U.S. at 353.

125. The reasonable expectation of privacy test is no longer the only viable path to demonstrating a Fourth Amendment search. In *United States v. Jones*, Justice Scalia's majority opinion revived the *Olmstead* trespass test, explaining that *Katz* did not displace the trespass test, while acknowledging that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." 565 U.S. 400, 411 (2012). And in *Florida v. Jardines*, Justice Scalia, writing for the majority, assessed the use of police dogs smelling for marijuana on the porch of a home under the trespass test. 569 U.S. 1, 6-9 (2013).

126. *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

127. *Id.* at 352 (majority opinion).

public telephone has come to play in private communication."[128] Ubiquitous public telephone use in 1960s America, along with the invasiveness of listening to the private words spoken within an enclosed booth, led the Court to conclude that withdrawing Fourth Amendment protection from the phone booth would inappropriately expand police power: Too many conversations that are too private would be denied constitutional protection.

Since *Katz*, the Court has continued to evaluate the Fourth Amendment implications of new consumer technologies from these two angles. In *Riley v. California*, the Court held that the warrantless search of a cell phone's contents incident to arrest is unreasonable and therefore barred by the Fourth Amendment.[129] Prior to *Riley*, searches incident to arrest were categorically exempt from the Fourth Amendment's warrant requirement under *United States v. Robinson*.[130] But as in *Katz*, the *Riley* Court recognized that the prevailing rule no longer maintained "the appropriate balance" between people and law enforcement, at least in the context of cell phones.[131] In reaching that conclusion, the *Riley* Court considered the same two dynamics the *Katz* Court did. The Court performed an unusually thorough analysis of the invasiveness of a cell phone search, concluding that "[m]odern cell phones . . . implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[132] The Court also reflected on the ubiquity of cell phone use and adoption, famously pointing out that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[133]

In *Carpenter*, the Court grappled with a more remote search related to a cell phone. The question presented was whether remote location monitoring of Mr. Carpenter's cell phone through cell-site location information (CSLI) gathered by his wireless carrier constituted a search under the Fourth Amendment.[134] As with each technology case before *Carpenter*, the Court made sure to assess the privacy interests at stake, acknowledging "the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach."[135] The Court also emphasized the ubiquity of cell phones, which amplifies the surveillance power of CSLI monitoring. The opinion began: "There are

128. *Id.*

129. *See* 134 S. Ct. 2473, 2485 (2014).

130. United States v. Robinson, 414 U.S. 218, 224 (1973).

131. *Riley*, 134 S. Ct. at 2484.

132. *Id.* at 2488-91.

133. *Id.* at 2484.

134. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

135. *Id.* at 2223.

396 million cell phone service accounts in the United States—for a Nation of 326 million people."[136]

But *Carpenter* was distinct from the Court's earlier technology cases because it fell at the intersection of cases about consumer-facing and police-facing technologies. The CSLI monitoring at issue in *Carpenter* was a product of both a new consumer technology (cell phones) and a new law enforcement tool for searching them. *Carpenter* was thus the Court's first true surveillance opinion. Justice Sotomayor's concurrence in *United States v. Jones* had raised the specter of surveillance, pointing out that "GPS monitoring [of a car] is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, . . . evad[ing] the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"[137] In *Carpenter*, the Court more fully embraced this issue. In assessing how the Fourth Amendment would respond to the way that "technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes,"[138] the Court added a third dimension to its analysis, evaluating the ease and scale of the surveillance made possible by CSLI monitoring technology. Echoing Justice Sotomayor's opinion in *Jones*, the Court emphasized that tracking location data had become "remarkably easy, cheap, and efficient," requiring "just the click of a button."[139] This analysis is fresh but not truly new. It is an application of the same inquiry into the balance of power between the state and its citizens that the Court has consistently engaged in since *Katz*, prompted by a technology that empowers the government to engage in surveillance like none the Court had evaluated before.

B. The Fourth Amendment and the Smart Home

Setting aside the specific doctrinal tests the Court may employ, the answer to the broader legal question—whether smart home data is entitled to Fourth Amendment protection—should be "yes." The Court has demonstrated that the contours of the Fourth Amendment are subject to change, especially when new technologies reshape the dynamic between people and police. Here, the profound intimacy of the data generated by smart home devices, the impending ubiquity of their adoption, and the ease and scope of the surveillance they enable compels Fourth Amendment protection.

---

136. *Id.* at 2211.

137. United States v. Jones, 565 U.S. 400, 415-16 (2012) (Sotomayor, J., concurring) (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

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

139. *Id.* at 2217-18.

The invasiveness of searching smart home device data is plain. Smart homes open a window into people's private lives as large as or larger than each technology to which the Court has already extended Fourth Amendment protection. In *Katz*, the Court was concerned about the police capturing private phone conversations made in public telephone booths.[140] Devices in the smart home can capture private conversations *made in private*, both with other people and with the devices themselves. In *Karo*, the Court held that tracking an individual's location within his home violates his reasonable expectation of privacy.[141] As the case studies discussed in Part I.C demonstrate, police can similarly use smart home data to reconstruct the movements of individuals throughout their homes. By combining the data—for example, when a given suspect opened the refrigerator, asked Alexa for the time, adjusted the thermostat, and turned on the TV—law enforcement can recreate not just a person's movements, but also her activities within her home. The inferences produced by police use of thermal imaging in *Kyllo* can be reproduced easily with the data from either a smart thermostat or smart energy meter.[142] Indeed, the vivid portrait of the resident's private life painted by the data collected by other devices discussed in Parts I.A and I.B surpasses anything the Court has ever considered.

The growing adoption of smart home devices provides additional reason to extend Fourth Amendment protections to the data they generate. It is projected that 20% of households will own smart devices by 2022,[143] and nearly 60% of Americans want them.[144] Already, more than 66 million adults are estimated to own smart speakers, including a 40% increase in ownership in 2018 alone.[145] Two-thirds of Americans are forecast to own a smart speaker by 2022.[146] And new homes are being built with these devices pre-installed.[147] If they haven't already, smart home devices are poised to permeate modern society, taking on an increasingly large role in modern life. To withhold Fourth Amendment protection from the data they generate would be to ignore the "vital role" they do and will play in society.[148]

---

140. Katz v. United States, 389 U.S. 347, 348-49 (1967).

141. United States v. Karo, 468 U.S. 705, 715-16 (1984).

142. *See* Natasha H. Duarte, *The Home Out of Context: The Post-*Riley *Fourth Amendment and Law Enforcement Collection of Smart Meter Data*, 93 N.C. L. REV. 1140, 1154-55 (2015).

143. Morrissey, *supra* note 15. This number does not include smart home speakers. *Id.*

144. GILLETT ET AL., *supra* note 16, at 3, 5 fig.1.

145. VOICEBOT & VOICIFY, SMART SPEAKER CONSUMER ADOPTION REPORT 3 (2019), https://perma.cc/M3RY-ULGS.

146. GILLETT ET AL., *supra* note 16, at 6 fig.2.

147. *See supra* note 38 and accompanying text.

148. *See* Katz v. United States, 389 U.S. 347, 352 (1967).

Carpenter's surveillance analysis further favors extending Fourth Amendment protections to the smart home. Police can obtain smart home data the same way they collect CSLI—from third-party companies. As with CSLI, such data can be called up with just a click. Surveillance of smart home data, much like the collection of CSLI, could be of alarming scope, empowering law enforcement to monitor not just one suspect's home, "but also everyone else's, not for a short period but for years and years."[149] The technology companies manufacturing smart home devices are, "[u]nlike the nosy neighbor who keeps an eye on comings and goings, . . . ever alert, and their memory is nearly infallible."[150] This level of surveillance is not perfect, but its scope far exceeds the "near perfect"[151] surveillance apparently implicated by CSLI collection. Like Winston's telescreen in *1984*, smart home devices may "receive[] and transmit[] simultaneously," rendering people "seen as well as heard" by the police.[152] And Justice Sotomayor's concerns about GPS technology, which echo the language of Orwell's dystopian writing, apply with special force to the surveillance of smart homes. "[B]y making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track," she feared, GPS technology "may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[153] What Justice Sotomayor feared as antithetical to the democratic society preserved by the Fourth Amendment is an Orwellian society in which people would have "to live . . . in the assumption that every sound [they] made was overheard, and, except in darkness, every movement scrutinized."[154]

George Orwell only conceived of a single telescreen surveilling the homes of the citizens of Oceania.[155] That concept was enough to conjure an image of surveillance so striking that it now serves as "*the* definitive statement of how a world without privacy would look."[156] The smart home has surveillance powers that eclipse even Oceania's. After all, Winston could evade the gaze of

149. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

150. *See id.*

151. *Id.* at 2218.

152. *See* GEORGE ORWELL, 1984, at 4 (1977 prtg.).

153. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *vacated mem.*, 565 U.S. 1189 (2012)).

154. *See* ORWELL, *supra* note 152, at 4-5.

155. *Id.* at 3-5 (describing the surveillance telescreen).

156. David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1076 n.27 (2014) (discussing *1984*'s frequent invocation in privacy scholarship).

his telescreen by hiding in an alcove.[157] As we continue placing sensors, cameras, and microphones into each room of our homes, the smart home may soon offer no such retreat.

III. Applying the Doctrine

Though a broad view of the Court's approach to the Fourth Amendment and technology suggests that smart home data is entitled to constitutional protection, courts must come to that conclusion by following or adjusting existing doctrine. The question whether smart home device data is entitled to Fourth Amendment protection raises several intersecting lines of Fourth Amendment jurisprudence. Because the data is generated from within the home, the Court's decisions exalting the home as the pinnacle of privacy are implicated. And because the intrusion into the home takes the form of a data request, we must also consider the Court's framework for evaluating data privacy, as articulated through a multidimensional analysis in *Riley*.[158] Most troublingly for claims to Fourth Amendment protection, smart home device data is often stored on third-party servers. Before *Carpenter*, that third-party storage led most to conclude that the case for constitutional protection is a nonstarter.[159] After *Carpenter*, the widely reviled rigidity of the third-party doctrine has been undermined, opening the door for extending Fourth Amendment protection to data voluntarily disclosed to third parties.

A. The "Firm Line" at the Entrance of the Home

The Fourth Amendment does not mention data.[160] It does not reference third parties.[161] But it explicitly protects the privacy of the home, drawing a "firm line" at the front door.[162] So we begin the constitutional analysis of searches of smart homes there, at the pinnacle of the Fourth Amendment's protections.

157. ORWELL, *supra* note 152, at 7.

158. *See* Riley v. California, 134 S. Ct. 2473, 2489-91 (2014) (examining the privacy implications of cell phone adoption from multiple angles).

159. *See, e.g.*, Duarte, *supra* note 142, at 1153; Ferguson, *supra* note 42, at 840; Burkett, *supra* note 9, at 1204-05; Boughman et al., *supra* note 9.

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

161. *See id.*

162. *See id.*; Payton v. New York, 445 U.S. 573, 590 (1980) ("[T]he Fourth Amendment has drawn a firm line at the entrance to the house.").

1. The sanctity of the home in Fourth Amendment jurisprudence

For the Supreme Court, the home is sacred. It is at the "core of the Fourth Amendment."[163] Police may not enter a home,[164] arrest a suspect at home,[165] move a stereo inside a home to look underneath it,[166] have a dog sniff the outside of a home,[167] or point a thermal imager at a home[168] without a warrant and probable cause. In the words of Stephanie Stern: "Homes have achieved iconic status in the modern Fourth Amendment, with judicial rhetoric elevating residential search to the apex of protection."[169]

The primacy of the home in Fourth Amendment jurisprudence is explained in part by its explicit inclusion in the text of the Fourth Amendment, whose vagaries otherwise frustrate scholars and Justices alike.[170] The Fourth Amendment provides, in relevant part: "The right of the people to be secure in their . . . houses . . . shall not be violated . . . ."[171] No test need be devised to divine the unambiguous commandment of our Founding Fathers that "[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[172]

The history points in the same direction. In a 1763 address in the House of Commons, William Pitt proclaimed:

> The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England cannot enter—all his force dares not cross the threshold of the ruined tenement![173]

That address "echoed and re-echoed throughout the Colonies."[174] Indeed, as the Court in *Payton v. New York* explained, "the overriding respect for the sanctity of the home . . . has been embedded in our traditions since the origins of the

163. Wilson v. Layne, 526 U.S. 603, 612 (1999).

164. Johnson v. United States, 333 U.S. 10, 17 (1948).

165. *Payton*, 445 U.S. at 601-03.

166. Arizona v. Hicks, 480 U.S. 321, 325 (1987).

167. Florida v. Jardines, 569 U.S. 1, 11-12 (2013).

168. Kyllo v. United States, 533 U.S. 27, 40 (2001).

169. Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905, 912 (2010).

170. *See supra* Part II.A.

171. U.S. CONST. amend. IV.

172. Payton v. New York, 445 U.S. 573, 589-90 (1980) (alterations in original) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

173. Miller v. United States, 357 U.S. 301, 307 (1958) (quoting William Pitt, Earl of Chatham).

174. *Payton*, 445 U.S. at 601 n.54.

Republic."[175] A search of the home "invades the precious interest of privacy summed up in the ancient adage that a man's house is his castle."[176] As the Court said in *Keith*, "physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed."[177]

Before *Katz*, the Court anchored Fourth Amendment protection to this history, evaluating its reach based on the common law of trespass,[178] which very clearly protected the home.[179] But even as the modern Fourth Amendment has purportedly come to protect "people, not places,"[180] the home has remained "inviolate."[181] One term after *Katz*, the Court clarified that *Katz* was not "intended to withdraw any of the protection which the Amendment extends to the home."[182] As the Court explained in *Payton*, in no setting "is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home."[183]

In *Kyllo*, the Court brought the Fourth Amendment home into the twenty-first century, holding that police use of a thermal imager to measure the heat emanating from Mr. Kyllo's home was a Fourth Amendment search.[184] Applying the *Katz* reasonable expectation of privacy test, the Court began with a strong presumption: "With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no."[185] The Court reasoned that a "search of the interior of homes" is the "prototypical and hence most commonly litigated area of protected privacy," so "[t]o withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."[186]

---

175. *Id.* at 601.

176. *Miller*, 357 U.S. at 307.

177. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 313 (1972).

178. *See* Olmstead v. United States, 277 U.S. 438, 465 (1928) ("The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted . . . ." (quoting Carroll v. United States, 267 U.S. 132, 149 (1925))), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

179. *See* 1 RESTATEMENT (FIRST) OF TORTS § 158 (AM. LAW INST. 1934) (describing unauthorized entry onto "land in possession of another").

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

181. Stern, *supra* note 169, at 906.

182. Alderman v. United States, 394 U.S. 165, 180 (1969).

183. Payton v. New York, 445 U.S. 573, 589 (1980).

184. Kyllo v. United States, 533 U.S. 27, 29, 40 (2001). The heat measured by the thermal imager revealed evidence of an indoor marijuana growing operation, which required high-intensity lamps. *Id.* at 29-30.

185. *Id.* at 31.

186. *Id.* at 34.

In addition to emphasizing the historical primacy of the home and the need to construe the Fourth Amendment sufficiently flexibly to keep pace with advancing technology, the *Kyllo* Court manifested a belief that the home is a place of special intimacy worthy of expansive privacy protections. "In the home," the Court wrote, "*all* details are intimate details, because the entire area is held safe from prying government eyes."[187] Setting aside the circularity of inferring that homes must be private because they are entitled to privacy, the Court's language evokes concern about the way that police observation of even ostensibly innocuous details emanating from people's homes may reveal deeply personal portraits of their lives. The *Kyllo* Court recognized that a thermal imager "might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate.'"[188]

2. The sanctity of the smart home

The Court's analysis maps clearly onto the data generated from within the smart home. Justice Scalia's invocation of the lady's bath was a clever demonstration of the intimacy of the information revealed by thermal imagers,[189] but it was perhaps the only clear example of how thermal imagers may reveal personal details about the resident. By contrast, virtually every detail about life at home may be captured by smart homes. And in the case of the lady taking the bath, along with revealing its timing, smart home devices could expose the temperature of the bath, which bottle of wine she took from the refrigerator, whether she dimmed the lights, and what music she listened to as she relaxed. The fact alone that such information is being generated from within the home, the apex of Fourth Amendment protection, militates in favor of bringing it within the Constitution's coverage. Indeed, "*all* details are intimate details" in the home,[190] and the smart home lays them bare.

Kyllo also offered a window into the way the enhanced privacy interests of the home interact with the third-party doctrine, discussed in more depth in Part III.C below. One of the principal arguments animating Justice Stevens's dissent was that Mr. Kyllo was not entitled to an expectation of privacy over information (or, in this case, heat) voluntarily revealed to the public.[191] This argument is the foundation for the third-party doctrine. As Justice Stevens suggested, "[w]hat a person knowingly exposes to the public, even in his

187. *Id.* at 37.

188. *Id.* at 38.

189. *See id.*

190. *Id.* at 37.

191. *See id.* at 42 (Stevens, J., dissenting).

own home or office, is not a subject of Fourth Amendment protection."[192] Though Justice Stevens stated the principle in absolute terms,[193] the *Kyllo* majority instructed us to treat it with more nuance. The Court rejected this "mechanical interpretation of the Fourth Amendment"[194] by making a purely consequentialist argument. A formalistic distinction between physical penetration of the home and surveillance through information that escapes the home's physical limits "would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home."[195] Any other finding would lead to a slippery slope that would end in the Court blinking as "ultrasound technology produces an 8-by-10 Kodak glossy."[196]

Applying this consequentialist argument to the smart home would favor bringing it within the ambit of Fourth Amendment protection. Just as heat emanates as radiation through the walls of a home, each piece of data from smart home devices leaves the home as electrons passing through wires or satellite signals. The volume and intimacy of the information captured by such devices looks like a logical extreme at the end of Justice Scalia's slippery slope, beyond what the Court had imagined possible in 2001, when a Kodak photo was the most invasive technological intrusion into the home it could conjure.

The key distinguishing feature between *Kyllo* and the smart home is that data from such devices does not emanate autonomously from the home in the way that heat emanated as a byproduct of Mr. Kyllo's use of high-intensity lamps. Though Mr. Kyllo voluntarily installed the heat lamps, he never explicitly agreed to the police thermally imaging the outside of his home.[197] By contrast, the owners of smart home devices traditionally agree to the data being stored elsewhere through user agreements.[198] Therefore, if law enforcement obtains smart home device data through the device's manufacturer, the traditional third-party doctrine analysis may continue to be implicated.[199] But if law enforcement obtains the data generated by the smart home in a way more analogous to *Kyllo*, such as through signal interference with the wireless networks that these devices may emit,[200] *Kyllo* likely

192. *Id.* (quoting California v. Ciraolo, 476 U.S. 207, 213 (1986)).

193. This expansive view of the third-party doctrine was the norm prior to *Carpenter*. *See infra* Part III.C.

194. *Kyllo*, 533 U.S. at 35 (majority opinion).

195. *Id.* at 35-36.

196. *Id.* at 36.

197. *See id.* at 29-31.

198. *See* Boughman et al., *supra* note 9.

199. *See infra* Part III.C.

200. *See* Ferguson, *supra* note 42, at 820-22.

compels a finding that such actions constitute a Fourth Amendment search and are therefore subject to a reasonableness requirement.

B. Assessing Digital Privacy in the Home Under *Riley*

Assessing a cell phone search for the first time, the Court in *Riley* developed a new rubric for evaluating the invasiveness of law enforcement searches of data. That framework, elaborated below, provides significant guidance for exploring the constitutionality of smart home searches.

1. *Riley*'s multifactor analysis

In *Riley*, the Court considered whether the search incident to arrest exception, which allows the police to perform warrantless searches of an arrestee, applies to searches of information stored on a cell phone.[201] The traditional exception was justified by the risk of harm to an officer and destruction of evidence during an arrest situation, along with a suspect's reduced expectation of privacy incident to arrest.[202] Under *Robinson*, the exception operated categorically, exempting searches from the warrant requirement even where those rationales were inapplicable.[203] Facing novel circumstances, the *Riley* Court carved out an exception to *Robinson*'s blanket exception to the warrant requirement, which may have struck the "appropriate balance in the context of physical objects," because its rationales—risk of harm to an officer, risk of evidence destruction, and reduced privacy expectations—did not have "much force with respect to digital content on cell phones."[204]

Riley's response to the first rationale, inapposite to our discussion of searches of smart home data, was that the risks of harm to officers and destruction of data considered inherent to arrest in *Robinson* are less pronounced when the search is of digital data.[205] In evaluating the second justification for the *Robinson* rule, the Court set out a new framework for evaluating the privacy interests implicated by devices that store or generate digital data. The Court concluded that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack," as in *Robinson*.[206] Suggesting searches of cell phones and cigarette packs were equivalent, as the government did, would be like saying "a

201. Riley v. California, 134 S. Ct. 2473, 2480 (2014).

202. *Id.* at 2484-88.

203. *See id.* at 2484-85; *see also* United States v. Robinson, 414 U.S. 218 (1973).

204. *Riley*, 134 S. Ct. at 2484-85.

205. *Id.* at 2484-88.

206. *Id.* at 2488-89.

ride on horseback is materially indistinguishable from a flight to the moon."[207] Though the Court seemed to consider the issue obvious, it took the time to provide a thorough analytical framework for establishing the heightened privacy interest implicated by cell phones. This analysis now serves as a useful guide to any assessment of whether certain devices or data are within the coverage of the Fourth Amendment.

To determine the invasiveness of a cell phone search, the *Riley* Court separately evaluated the breadth, depth, and intimacy of the data stored in cell phones, the length of time for which data is available, and the pervasiveness of the technology.[208] Though the nexus for much of the Court's analysis was the cell phone's storage capacity, the Court gave weight to it only insofar as it related to the factors above.[209] Therefore, the analysis should apply to devices that implicate the same data privacy concerns without "immense storage capacity."[210] Considering these factors and the Court's specific analysis with respect to cell phone data, I contend that the grounds for extending Fourth Amendment protection to smart home data are no less obvious.

2. *Riley* and the smart home

First, the Court considered the breadth of information stored on and generated by cell phones. Cell phones, the Court noted, may contain "photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on."[211] The wide array of data stored on cell phones implicates privacy concerns both because that information is especially intimate and because it "reveal[s] much more in combination than any isolated record."[212] The Court's recognition of the "mosaic effect"[213] is a critical development in its privacy jurisprudence. It opens the door to extending Fourth Amendment protection to devices or data that generate or aggregate vast sums of data that collectively raise privacy concerns by combining information "in unexpected ways, giving rise to powerful inferences."[214] This potential aggregation is the precise danger posed by searches of smart home data.[215] Any individual data point captured by a

207. *Id.* at 2488.

208. *Id.* at 2489-90.

209. *See id.* at 2489-91.

210. *See id.* at 2489.

211. *Id.*

212. *Id.*

213. *See supra* Part I.C.

214. *See* Peppet, *supra* note 65, at 120.

215. *See supra* notes 63-69 and accompanying text.

sensor in one's home may prove harmless from a privacy standpoint.[216] But the smart home is an interconnected space where data is continuously generated and combined by many devices, creating a mosaic effect even more potent than the one examined in *Riley*.

The Court also emphasized the intimacy of the data stored on cell phones. "An internet search and browsing history," the Court points out, "could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD."[217] Certainly, a query about a health condition to Alexa could reveal the same information. The data generated by a smart pill bottle could be even more invasive. And as health applications for smart home technology continue to develop,[218] the depth of medical data collected within the smart home will far exceed that available through a cell phone, except to the extent the cell phone contains apps linked to the smart home.

The Court proceeded to describe the multitudinous apps available on cell phones and the sensitive information they generate. These apps, the Court feared, could offer revelations about political and religious associations, medical information such as whether the user is pregnant, and other private data.[219] Much of the same information, and many other details unique to the home, are revealed by ordinary devices in the modern smart home. Smart TVs may capture political preferences.[220] Alexa may hear personal battles with mental health.[221] A smart pill bottle full of prenatal vitamins or a fridge that reveals certain patterns or changes in its contents may hint at a pregnancy. And whatever information is stored on a given person's cell phone can often be called up through the devices of the smart home.[222]

Smart homes, like the cell phones analyzed in *Riley*, also produce data with immense depth and reach in time. "The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions . . . ."[223] So too with a compilation of the individual's every interaction with a smart home assistant, or years of footage from an in-home or doorbell camera, stored indefinitely on companies' servers.

---

216. Though, as the Court declared in *Kyllo*, in the "sanctity of the home," "*all* details are intimate details." Kyllo v. United States, 533 U.S. 27, 37 (2001).

217. *Riley*, 134 S. Ct. at 2490.

218. *See supra* text accompanying notes 39-41.

219. *Riley*, 134 S. Ct. at 2490.

220. *See supra* notes 27-28 and accompanying text.

221. *See supra* text accompanying note 61.

222. *See supra* text accompanying notes 31-34.

223. *Riley*, 134 S. Ct. at 2489.

And while cell phone ownership still far exceeds smart home adoption,[224] the number of smart devices is already staggering and on the rise. Smart homes are poised to be a pervasive feature of the modern home. As these technologies continue to be purchased and even built into new homes, the "proverbial visitor from Mars" will be right to conclude that such devices are an "important feature of [the home's] anatomy."[225]

C. The Third-Party Problem

Most who have considered this issue have assumed smart home data stored on third-party servers, however intimate, lies outside the Fourth Amendment's protection.[226] Before *Carpenter*, the third-party doctrine was generally viewed as categorical, and often portrayed as such by the Court.[227] In *Carpenter*, however, the Court dispelled the myth that the third-party doctrine sweeps so broadly. How and to what extent this move should and will reshape Fourth Amendment doctrine is an open question. I contend that *Carpenter*'s approach to bending the third-party doctrine in response to new technology opens the door to extending the Fourth Amendment's protections to sensitive information stored on third-party servers, including smart home data. I also contend the Court did not go far enough and should abandon its "assumption of risk" approach to evaluating third-party doctrine cases.

1. The third-party doctrine

The third-party doctrine may be the most reviled Fourth Amendment canon. Voluntary disclosure decisions "top[] the chart of [the] most-criticized [F]ourth [A]mendment cases."[228] As Orin Kerr put it, "[a] list of every article or book that has criticized the doctrine would make [for] the world's longest law review footnote."[229] The panning has only intensified as scholars recognized "[t]he third-party doctrine [as] one of the most serious threats to privacy in the digital age."[230] Even before *Carpenter*, the Court has declined to offer much

224. *Compare id.* at 2490 (commenting that "90% of American adults . . . own a cell phone"), *with* GILLETT ET AL., *supra* note 16, at 3, 6 fig.2 (projecting that 20% of American households will own smart devices and 50% will own smart speakers by 2022).

225. *See Riley*, 134 S. Ct. at 2484.

226. *See supra* note 159 and accompanying text.

227. *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976).

228. *See* 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).

229. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 n.5 (2009) (collecting examples of scholars criticizing the third-party doctrine).

230. *See* Daniel J. Solove, Essay, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005).

defense for the doctrine beyond asserting that those who share information with a third party "assume[] the risk"[231] that it will end up in the wrong hands.[232] Of course, that rationale is circular. There would be no risk to assume if the law continued to protect the information after its disclosure.

The third-party doctrine developed through two related lines of cases: one about undercover agents,[233] the other about business records.[234] The Court has long held in cases featuring suspects revealing information to undercover agents or informants that the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[235] In *United States v. White*, the Court extended the doctrine into the post-*Katz* era by refusing to recognize an expectation of privacy in information voluntarily disclosed to another person.[236] "Inescapably," Justice White's plurality opinion insisted, "one contemplating illegal activities must realize and risk that his companions may be reporting to the police."[237]

In cases about business records, the Court drew the same line. In *United States v. Miller*, the defendant challenged the government's subpoena of his bank records without a warrant.[238] The Court suggested the documents were not personal, but rather were ordinary financial documents.[239] Citing *White*, the Court reaffirmed that the defendant in *Miller* "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[240] Therefore, the Court held, the "Fourth Amendment does not prohibit" obtaining information conveyed to a third party "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[241] Shortly after *Miller*, the Court reached the same conclusion for

231. Smith v. Maryland, 442 U.S. 735, 744 (1979).

232. *See* Carpenter v. United States, 138 S. Ct. 2206, 2263 (2018) (Gorsuch, J., dissenting) ("What, then, is the explanation for our third party doctrine? The truth is, the Court has never offered a persuasive justification.").

233. *See, e.g.*, Hoffa v. United States, 385 U.S. 293 (1966).

234. *See, e.g.*, United States v. Miller, 425 U.S. 435 (1976).

235. *Hoffa*, 385 U.S. at 302.

236. *See* 401 U.S. 745, 752 (1971) (plurality opinion).

237. *Id.*

238. 425 U.S. at 436.

239. *Id.* at 442.

240. *Id.* at 443 (citing *White*, 401 U.S. at 751-52 (plurality opinion)).

241. *Id.* (citing *White*, 401 U.S. at 752 (plurality opinion)).

the same reasons in two other business records cases, *Couch v. United States*[242] and *United States v. Payner*.[243]

In *Smith v. Maryland*,[244] the burgeoning third-party doctrine was put to the test in a new context and came out stronger than ever. *Smith* presented the question whether installation of a "pen register" that recorded the numbers dialed from the defendant's home constituted a Fourth Amendment search.[245] The Court made sure to distinguish the case from *Katz*, noting that a pen register is different from a recording device because it "do[es] not acquire the *contents* of communications,"[246] perhaps suggesting that the privacy interests implicated by the purported search influence the third-party doctrine analysis. The Court was also sure to emphasize that the disclosure of the dialed phone number was knowing and voluntary, suggesting that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[247] Thus, citing the defendant's assumption of risk, the Court declined to recognize the defendant's claimed expectation of privacy as objectively reasonable: "[I]t is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."[248]

2. *Carpenter* and the smart home

In *Carpenter*, the Court struck a profound blow to the reach of the third-party doctrine. Though commentators had long treated the third-party doctrine as a categorical rule sweeping all voluntarily disclosed information outside the reach of the Fourth Amendment, the *Carpenter* Court downplayed the force of *Smith* and *Miller* and eschewed "mechanically applying the third-party doctrine" to *Carpenter*'s facts.[249]

---

242. 409 U.S. 322 (1973).

243. 447 U.S. 727 (1980).

244. 442 U.S. 735 (1979).

245. *Id.* at 736.

246. *Id.* at 741.

247. *Id.* at 742.

248. *Id.* at 743-44.

249. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018). The *Carpenter* Court did not address, distinguish, or otherwise limit the undercover agent cases. But nothing in *White* or *Hoffa*—or the Court's subsequent precedent—suggests either that the third-party doctrine operated differently in the undercover agent context than in the business records context or that it would after *Carpenter*. Dissenting in *Carpenter*, Justice Gorsuch noted that consent-based justifications for the third-party doctrine are more persuasive in the government agent context. *Id.* at 2263 (Gorsuch, J., dissenting). But, as relevant here, Justice Gorsuch also emphasized that "[c]onsenting to give a third

footnote continued on next page

The Court carved out CSLI data from the third-party doctrine by carefully examining the rationales for the doctrine and demonstrating their inapplicability to CSLI collection.[250] With regard to the first rationale, that "an individual has a reduced expectation of privacy in information knowingly shared with another," the Court retorted that "the fact of 'diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely.'"[251] According to the *Carpenter* Court, *Smith* emphasized the "limited capabilities of a pen register."[252] And *Miller* "noted that checks were 'not confidential communications.'"[253] The Court suggested that "when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying . . . a detailed and comprehensive record of the person's movements."[254] The government's arguments for extending the third-party doctrine to CSLI thus "fail[ed] to contend with the seismic shifts in digital technology that made possible" tracking the defendant's location at all times.[255] As in *Riley*, where the Court refused to extend a categorical rule because cell phones implicate more profound privacy concerns than cigarette boxes, the *Carpenter* Court declined to apply the third-party doctrine to CSLI because of the "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."[256]

If the Court ended its analysis there, the case for Fourth Amendment protection of smart home data would be a slam dunk. Surely there is a similarly large "world of difference" between business records or dialed phone numbers and the "exhaustive chronicle" of private details about people's private lives collected by smart home devices. The privacy interests implicated by police access to smart home data far outweigh those raised by long-term CSLI tracking.[257] Not only can the smart home relay information about a person's location in the world—by revealing whether they are at home or not—it may also convey the resident's location within her own home, the precise form of information-gathering held unconstitutional in *Karo*. That is not to mention

---

party access to private papers that remain my property is not the same thing as consenting to a *search of those papers by the government.*" *Id.*

250. *See id.* at 2219-20 (majority opinion).

251. *Id.* at 2219 (quoting Riley v. California, 134 S. Ct. 2473, 2488 (2014)).

252. *Id.*

253. *Id.* (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

254. *Id.* at 2217.

255. *Id.* at 2219.

256. *Id.*

257. *See supra* Part II.B.

the myriad other sensitive details captured by smart home devices, discussed throughout this Note.

But the Court did not stop at the first rationale. Instead, it also insisted that the "second rationale underlying the third-party doctrine—voluntary exposure—[does not] hold up when it comes to CSLI."[258] The Court contended that CSLI is not "truly 'shared' as one normally understands the term."[259] Here, the Court made its most radical departure from the reasoning of *Smith*. If it was "too much to believe" that telephone users in the 1970s did not understand that the phone number they dialed was transmitted to the telephone company,[260] it seems similarly unlikely that cell phone users are not aware that their calls are made by connecting the phone to cell towers that can triangulate the phone's general location. For decades, popular media has been rife with examples of precisely that image—an officer getting a suspect on the line and tracing the suspect's location.[261] That is not to mention that more than 50% of Americans use their cell phones for GPS navigation.[262] The *Smith* Court's approach would suggest they should be aware that their location is being transmitted to the company behind the GPS app so that it can determine which detailed maps and live traffic information to download.

In *Carpenter*, the Court flipped the presumption, noting that cell phones transmit location information "without any affirmative act on the part of the user beyond powering up."[263] Anticipating the obvious additional response that purchasing a phone and using it daily is a voluntary, affirmative act, the Court adopted a narrower conception of consent. Because "carrying [a cell phone] is indispensable to participation in modern society," the Court concluded that cell phone users do not meaningfully consent to transmission of location data.[264]

By adopting this fiction of nonconsent, the Court preserved the assumption-of-risk rationale of the third-party doctrine. Whether or not litigants must defeat both the privacy and assumption-of-risk rationales of the

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

259. *Id.*

260. Smith v. Maryland, 442 U.S. 735, 743 (1979).

261. *See* Jay MacDonald, *Can Police Really Trace a Call in 60 (but Not 59) Seconds?*, FOX BUS. (Apr. 21, 2011), https://perma.cc/NZQ2-3R9M ("It's a Hollywood plot device as old as the Princess phone: The good guys receive a call from the kidnapper/mad bomber/drug lord, they need to string him along for 60 seconds to trace the call, but he's wise to their time constraint and hangs up just short of the one-minute mark.").

262. Alexander Kunst, *Share of Americans Who Used Their Cell Phone for Online Map or Navigation Services in the Last Four Weeks in 2018, By Age*, STATISTA (Sept. 3, 2019), https://perma.cc/LZS6-6CA9.

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

264. *See id.*

third-party doctrine after *Carpenter* is unclear.[265] If both rationales must be demonstrated inapplicable, defendants seeking to suppress the fruits of a smart home search will face an uphill battle. Though they are incredibly pervasive, smart home devices are not truly "necessary" to modern life. The majority of Americans do not own smart home devices and get along just fine without them. Whoever buys those devices despite the Orwellian media coverage about them surely does so voluntarily, even if users are not always aware the data ends up on third-party servers. And while each of the nine Supreme Court Justices likely owns a cell phone like the ones at issue in *Riley* and *Carpenter*, they may react incredulously to the idea of voluntarily bringing an "always on, always listening" smart home assistant into their homes.

3. A path forward

The *Carpenter* Court took care to retain the third-party doctrine and its traditional justifications while refusing to accept the unconscionable outcome that constant real-time location monitoring would not be considered a search under the Fourth Amendment. By effectively exempting CSLI from the third-party doctrine, the Court served the Fourth Amendment's purpose to "place obstacles in the way of a too permeating police surveillance."[266] But retaining the third-party doctrine, endorsing its widely rebuked rationales, and limiting the decision to CSLI is too weak an obstacle to digital surveillance. Recognizing the boundless potential for surveillance in the digital age, where sensitive data is constantly turned over to third parties, should have led to a more forceful, better reasoned departure from the third-party doctrine.

Carpenter's view of assumption of risk is a poor foundation for reshaping Fourth Amendment jurisprudence to the realities of the modern era. Its reasoning is flawed, produces unreasonable outcomes, and is at odds with the Court's broader jurisprudence. As discussed above, the assumption-of-risk rationale is circular. The Court's adoption of a fiction of nonconsent in *Carpenter* raises additional quandaries. For one thing, the Court has not viewed consent so mercifully in other contexts, either civil or criminal. Parties to a

265. For example, in a case challenging a public utility's compulsory collection of residential electricity usage data through "smart meters," the Seventh Circuit appeared to address the third-party doctrine only by responding to the assumption-of-risk rationale. *See* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018). Citing *Carpenter*, the court concluded that "a home occupant does not assume the risk of near constant monitoring by choosing to have electricity in her home." *Id.* Notably, the court had already found that electricity usage monitoring invaded a privacy interest but did not relate that discussion to its dismissal of the third-party issue. *See id.* at 526-27.

266. *See* United States v. Di Re, 332 U.S. 581, 595 (1948).

contract need not read its terms to be bound by it.[267] Defendants consistently struggle to show they did not waive their *Miranda* rights voluntarily and knowingly.[268] It is exceedingly hard to imagine the Court in other contexts accepting the argument that a party to an agreement did not assent because they felt they had no choice as a result of everyone else signing it. Employment contracts are enforced though working is a necessity of modern life, even against laborers without other meaningful options for making a living.[269] The Court would certainly not endorse a party to a cell phone contract reneging on its terms on the grounds that "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[270] That the Court chose to depart so radically from its traditional view of consent here demonstrates its discomfort with the results of "mechanically applying"[271] the assumption-of-risk rationale in high-privacy contexts. As I will argue, this discomfort should lead the Court to abandon the rationale as an independent reason to deny people the Fourth Amendment's protections.

Smart home devices provide a forceful illustration of a second logical defect in the *Carpenter* Court's efforts to preserve the assumption-of-risk rationale. If the pervasiveness of a technology is a measure of whether people meaningfully consent to using it, drawing a line distinguishing "pervasive therefore necessary" from "common but inessential" technologies will be impossible. In addition to the line-drawing issue it creates, a "necessity to modern life" approach to assessing assumption of risk is misguided. For example, though smart home device adoption grows dramatically with each year, smart home technology is not yet truly indispensable to participation in modern society. If the assumption-of-risk rationale is in play after *Carpenter*, it won't be until smart home devices are built into most every modern home that the Fourth Amendment will apply. This dynamic illustrates the central flaw of this approach. Things become a necessity of modern life through ubiquitous voluntary acceptance over time. We collectively and individually consent to privacy tradeoffs to acquire the benefits of technology. Devices only become necessary to modern life because people have widely assumed the risk of their adoption. Yet, ignoring reality, the Court in *Carpenter* relies on the resulting

267. *See* Charles L. Knapp, *Is There a "Duty to Read"?*, 66 HASTINGS L.J. 1083, 1085-86, 1088-89 (2015).

268. *See, e.g.*, Berghuis v. Thompkins, 560 U.S. 370, 382-89 (2010).

269. *See, e.g.*, Walthour v. Chipio Windshield Repair, LLC, 745 F.3d 1326, 1327-28, 1337 (11th Cir. 2014) (affirming an order enforcing a group of window repairers' individual arbitration agreements and dismissing their collective suit).

270. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (quoting Riley v. California, 134 S. Ct. 2473, 2484 (2014)).

271. *Id.* at 2219.

"indispensable" quality of cell phones—really, another word for ubiquity—to claim we do not meaningfully consent to sharing our data.[272] In effect, the Court's current approach would be to deny people Fourth Amendment protections because they have assumed the risk of adopting a technology until so many people have assumed the risk that the Court relents, adopting a fiction to declare the widespread, voluntary adoption of the technology nonconsensual.

The smart home also demonstrates the patent unfairness of punishing people for adopting consumer technologies that undermine their privacy in ways they cannot and do not understand. To the extent consumers understand that purchasing useful gizmos for their home constitutes voluntary disclosure of their most sensitive data to a third party, they may not know the path their data will follow because of companies' opaque data-sharing policies. In many cases, apps share exceedingly private data with other companies without a way for the user to opt out.[273] It defies reality to suggest that people consent to such third-party disclosure more meaningfully than to the transmission of their location directly to their cell phone service provider.

A better approach is to abandon assumption of risk as an independent barrier to Fourth Amendment protection and fold the voluntary disclosure analysis into the standard Fourth Amendment "reasonable expectation of privacy" test. In doing so, the Court could do away with the third-party doctrine as a standalone bogeyman and bring situations featuring voluntary disclosure into alignment with its prevailing test for whether an action is a search. The Court has recognized since *Katz* that people have a reduced expectation of privacy over information knowingly disclosed to third parties or the public.[274] Indeed, in many cases, the privacy interests implicated by a category of technology measured against the voluntariness of people's data disclosure will militate against extending Fourth Amendment protection. But to categorically refuse to apply the Fourth Amendment when the disclosure was voluntary is illogical and devastating to privacy in modern society. It should be sufficient to demonstrate that an individual maintained an objectively reasonable expectation of privacy over the information despite voluntarily disclosing it to a third party.

IV. Rethinking Privacy in the Home

Much of this Note's analysis of the Fourth Amendment questions raised by smart home adoption has taken for granted a basic premise: We are entitled to

272. *See id.* at 2220.

273. *See supra* notes 46-47 and accompanying text.

274. *See* Katz v. United States, 389 U.S. 347, 351-52 (1967); *see id.* at 361 (Harlan, J., concurring).

a reasonable expectation of privacy within our smart homes. Given the Court's unwavering affirmation of the home's sanctity,[275] that assumption may seem reasonable. But given that expectations of privacy must be objectively reasonable to obtain constitutional stature, it is an assumption worth exploring. As a prominent privacy scholar has pondered: "Once your home is turned inside out, does [your] reasonable expectation of privacy dissipate?"[276]

This Part contends that it should not. To be sure, certain forms of privacy in the home, such as control over information generated from within the home, may be eroded—perhaps eviscerated completely—by adoption of smart home technology. But other dynamics of privacy—namely, privacy as refuge—are intensified by the smart home, a source of technologically enriched refuge no less worthy of Fourth Amendment protection.

A. The End of Privacy in the Home?

Privacy scholars and science fiction authors alike have viewed technology with suspicion for decades. To many, the rise of consumer technology and the surveillance state signals the end of days for any meaningful sense of privacy. As a prominent technology CEO infamously put it in 1999: "You have zero privacy anyway. Get over it."[277] Some scholars have set out to develop a theory of the Fourth Amendment untethered to the concept of privacy, reflecting "a world without privacy."[278] Perhaps the most influential death-of-privacy prognosis came from futurist David Brin. In *The Transparent Society*, Brin argued forcefully that our attempts to salvage privacy are doomed: "[I]t is already far too late to prevent the invasion of cameras and databases. . . . No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases. They are here to stay."[279]

But even Brin, among the fiercest of privacy doomsday theorists, did not anticipate private or government surveillance reaching into the home. Even in the most extreme world of surveillance Brin could imagine, people would retain a baseline level of "bedroom privacy."[280] Even as "camera-bearing robots may swarm the skies," there will remain "a realm that each of us calls deeply

275. *See supra* Part III.A.1.

276. Astor, *supra* note 23 (quoting Albert Gidari, Director of Privacy, Stanford Center for Internet and Society).

277. Polly Sprenger, *Sun on Privacy: "Get Over It,"* WIRED (Jan. 26, 1999, 12:00 PM), https://perma.cc/9HKU-PYSZ (quoting Scott McNealy, CEO, Sun Microsystems).

278. *See, e.g.*, Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1320 (2012).

279. DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 8-9 (1998).

280. *See id.* at 269.

personal, wherein we seek either solitude or intimacy."[281] That is, a "place to hold things we want kept private."[282]

It turns out that even David Brin underestimated the destruction of privacy made possible less than twenty years after he published *The Transparent Society*. Surveillance drones may not regularly patrol the skies just yet,[283] but cameras, microphones, and other sensor-equipped devices already surveil our homes and bedrooms. And we're putting them there ourselves.

The home was supposed to remain the final vestige of our privacy. In the grimmest visions of a transparent future, the home remained the last zone of refuge free from prying eyes. In the age of the smart home, even that hope has been dashed.

B. Home as Technologically Enriched Refuge

My view is not so bleak. I contend that the smart home only eviscerates one form of privacy in the home: informational privacy. Building on David Sklansky's conception of "privacy as refuge,"[284] I contend that smart home devices require a reimagining of the home as a place of technologically enriched refuge. Whether or not data about people's home lives is stored on third-party servers, smart home technology is not tearing down the walls of the home. Rather, it is redefining the way that people interact with their foremost source of refuge. The home is no less worthy of privacy because it has become "smart." To the contrary, smart home devices intensify the privacy to which homes have always been traditionally entitled.

1. Informational privacy

Informational privacy refers to one's control over data flows. In the pre-digital age, control over dissemination of information about oneself could be viewed as but one of the many dimensions composing the concept we call privacy. Today, discussions of privacy inevitably revolve around control over information. Indeed, in the digital era, the word "privacy" generally refers to privacy over a certain piece or source of information. This reality is reflected in popular media, legal scholarship,[285] and the Court's modern

281. *Id.* at 269-70.

282. *Id.* at 270.

283. At least not the sort of surveillance drones imagined by Brin. Perhaps that reality is not far off either. *See Surveillance Drones*, ELECTRONIC FRONTIER FOUND., https://perma.cc/46PA-SYQ4 (archived Nov. 10, 2019).

284. *See* Sklansky, *supra* note 156, at 1113.

285. *Id.* at 1083-84 (summarizing the legal scholarship's shift to a focus on informational privacy).

decisions.[286] In April 2019, the *New York Times* began publishing *The Privacy Project*, a series of articles and interactive pieces (over one hundred, as of November 2019) exploring privacy and technology.[287] The articles consistently rely on a view of privacy as control over information, from genetic and biometric data to social media and location information.[288] This data-oriented view of privacy "has become 'the cornerstone of our modern right to privacy.'"[289]

To the extent technology truly threatens to bring about the death of privacy, it is only informational privacy that risks extinction. As Sklansky points out, "[t]hat point tends to get lost because of the assumption, unstated but ever more prevalent, that privacy *is* informational privacy."[290] As people, companies, and police adopt new technologies, we generate ever more vast amounts of data that are ripe for surveillance and manipulation by private or public third parties. People are plagued by the sense that they have lost control over information they once considered sensitive. Indeed, 91% of Americans surveyed revealed feeling they lacked control to some extent over how their personal information was collected and disseminated.[291] Likewise, this Note focuses primarily on the volume and intimacy of information generated and disseminated by smart home devices as a measure of their privacy implications. That approach is partially the result of the need to speak in terms of informational privacy to comport with the Supreme Court's framework for evaluating privacy interests. It is perhaps also a reflection of the privacy dynamic most threatened by widespread adoption of the smart home. But informational privacy is not the only conception of privacy at play.

2. Privacy as refuge

Informational privacy lacks explanatory power for the substance of what we consider private. "[C]ontrol over personal information" is but one of six conceptions of privacy identified by Daniel Solove.[292] Indeed, not all

286. The Court in *Riley*, *Carpenter*, and *Jones* evaluated claims of Fourth Amendment protection over information.

287. *The Privacy Project*, N.Y. TIMES, https://perma.cc/GV2D-4BJR (archived Nov. 10, 2019).

288. *Id.*

289. Sklansky, *supra* note 156, at 1083 (quoting Margalit Fox, *Alan F. Westin, Who Transformed Privacy Debate Before the Web Era, Dies at 83*, N.Y. TIMES (Feb. 22, 2013), https://perma.cc/L5MJ-TZPC).

290. *Id.* at 1088.

291. A.W. Geiger, *How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks*, PEW RES. CTR.: FACT TANK (June 4, 2018), https://perma.cc/2J2N-LTJ8.

292. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV 1087, 1092 (2002) (arguing that privacy can be conceived of as a right to be let alone, limited access to oneself, secrecy,
footnote continued on next page

information is fairly characterized as private. That alone suggests that privacy as "control over information" is to some extent question-begging, relying "on some independent notion of what is 'private' or 'personal.'"[293] If "certain information is private or personal, it is presumably because it relates to certain actions, places, or relationships that are themselves private or personal."[294] This critique, advanced by David Sklansky, highlights two dimensions along which informational privacy is lacking. First, it "must rely on some independent notion" of what constitutes "private" information.[295] Second, it does not capture the range of ways that privacy is violated outside of the misuse of private data.[296] The paradigmatic example, Sklansky argues, is the strip search. Despite the well-established "sense that strip searches are particularly invasive and require particularly strong justification," the "focus on informational privacy has made it increasingly difficult to discern what is exceptional or extreme about strip searches."[297] It is uncontroversial to suggest that what makes a strip search violate privacy goes beyond the "information" about the victim's physical appearance being exposed to another party. Similarly, physical intrusions into the home are especially invasive not because information about furniture arrangements inside of the dwelling is a profound secret. Such intrusions violate privacy because they invade a sphere of personal sovereignty.

To better account for the underlying question of what is private, and why strip searches and home invasions violate it, Sklansky suggests the framework of privacy as refuge, "respect for a personal sphere shielded, but not completely immune, from public inspection and regulation."[298] This conception of privacy, endorsed by others suspicious of informational privacy's explanatory power,[299] captures the need for an "oasis, some shelter from public scrutiny, some insulated enclosure, some enclave, some inviolate place"[300] we associate with privacy. Privacy as refuge accords with the way we view the home and

control over personal information, personhood (control of one's personality), and intimacy).

293. *See* Sklansky, *supra* note 156, at 1102.

294. *Id.*

295. *Id.*

296. *See id.* at 1102-03.

297. *Id.* at 1103.

298. *Id.* at 1113.

299. *See, e.g.*, Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425, 452-53 (2017) (noting that "an approach to privacy that focuses too heavily on information streams" could "push[] arguably higher-stakes privacy invasions to the margins and privilege[] data over bodies").

300. Silverman v. United States, 365 U.S. 505, 511 n.4 (1961) (quoting United States v. Lee, 193 F.2d 306, 315-16 (2d Cir. 1951) (Frank, J., dissenting), *aff'd*, 343 U.S. 747 (1952)).

body as spaces over which we are sovereign, giving content to the concept of privacy and better explaining the intrusiveness of privacy-violating actions beyond information dissemination. It is also the precise vision for privacy maintained even by the most ardent privacy doomsday thinker: In David Brin's transparent society, there must be "some zone of sanctuary where we can feel unobserved[,] [s]ome corner where our hearts can remain forever just our own."[301]

Among the reasons to favor privacy as refuge, according to Sklansky, is that it "makes clear why privacy should not be written off as dead or dying."[302] Writing in 2014, he noted that "most of us still have a place we can go where we are shielded from public scrutiny and government surveillance."[303] Five years later, does the rise of the smart home mean the death of this vision of privacy too?

Not so. People with the good fortune to have a home and fill it with technology still come back to it every day from work or school and enjoy the zone of seclusion offered by the four walls and roof over their heads. The roving Roomba vacuum may free up more time to watch television or read, but it does not shatter the sense of intimacy and privacy one innately feels at home. Regardless of the data being generated from within, the home remains an enclave in which we feel especially safe and sovereign. Buying a smart home assistant or smart refrigerator does not make a home invasion or robbery less painful. Intrusions into our private space disturb our sense of privacy because they infringe on our walled-off, sovereign sphere of intimacy and seclusion. For the same reasons that the informational privacy framework does not capture the invasiveness of a strip search, the rise of smart home technology cannot mean the death of privacy as refuge in the home.

To the contrary, the smart home makes home a source of even greater refuge and therefore of heightened privacy. Though they generate vast sums of data and detract from our informational privacy, smart home devices expand the range of activities available to us within our homes. They equip the home to handle profoundly private interactions with its resident, enhancing the zone of seclusion into a sphere of boundless intimate dynamics between people and their technologies. A crucial feature of our "zones of refuge" is the intimacy they afford to people within them.[304] The smart home injects a new flavor of intimacy into the home. Researchers have already begun examining the dynamics of companionship implicated by ownership of smart home

301. BRIN, *supra* note 279, at 270.

302. Sklansky, *supra* note 156, at 1114.

303. *Id.*

304. *See id.* at 1108-09.

devices.[305] Smart home residents can cook with their smart kitchens, asking for suggested recipes and guidance on tricky culinary techniques.[306] They can sing to songs suggested by Alexa and have dance parties on their virtual reality headsets.[307] They can tell their devices "good morning" and "good night." They are empowered to reveal details about their health and physiology and obtain medical advice not unlike that provided within a doctor's office, a canonically private place.[308] People already treat smart home assistants as confidantes and friends, relying on them primarily for interactions outside of the core functionalities for which they were designed.[309] Alexa users convey their inner life to their devices, expressing mental health struggles and even thoughts of suicide, evidence of the refuge people seek and find in the smart home.[310] As the technologies develop, our personal relationship with our smart homes will continue to evolve. Amazon's technologists promise that before long, "a conversation with a digital assistant will be indistinguishable from one with a person."[311] For the elderly, the smart home is already a powerful source of companionship and assistance.[312] A lonely retiree in Oakland, California, describes his robotic assistant as his "little blue-eyed girlfriend."[313] "She keeps me on my toes," he says.[314]

The smart home began as a source of convenience. Voice-controlled lights, flashing pill bottles, and autonomous vacuums save time and simplify life at home. But the future of the home blends convenience with intimacy and companionship. It answers the calls of a lonely generation,[315] enabling people to seek refuge in the home in new, more intimate, ways. This technologically

305. *See, e.g.*, Byounggwan Lee et al., *Companionship with Smart Home Devices: The Impact of Social Connectedness and Interaction Types on Perceived Social Support and Companionship in Smart Homes*, 75 COMPUTERS HUM. BEHAV. 922 (2017).

306. *See* Molly Price, *Whirlpool, GE and the Dozens of Cooking Apps Crowding the Smart Kitchen*, CNET (Jan. 19, 2019, 5:00 AM PST), https://perma.cc/3ZGL-D2DF.

307. *See* Michael McWhertor, *Dance Central Goes VR for Oculus Quest and Rift*, POLYGON (Mar. 27, 2019, 11:00 AM EDT), https://perma.cc/BK8Q-STTF; Chris Welch, *Alexa Can Now Find the Right Amazon Music Playlist by Having a Conversation with You*, VERGE (Dec. 6, 2018, 9:00 AM EST), https://perma.cc/2DSW-A5L8.

308. *See supra* text accompanying notes 39-41.

309. *See supra* notes 60-62 and accompanying text.

310. *See supra* text accompanying note 61.

311. Stevens, *supra* note 62.

312. *See* Imani Moise, *For the Elderly Who Are Lonely, Robots Offer Companionship*, WALL ST. J. (May 28, 2018, 10:01 PM ET), https://perma.cc/QM93-5HCA.

313. *Id.*

314. *Id.*

315. *See* Rhitu Chatterjee, *Americans Are a Lonely Lot, and Young People Bear the Heaviest Burden*, NPR: SHOTS (May 1, 2018, 6:01 AM ET), https://perma.cc/JEB9-JSXF.

enhanced refuge is a reimagining of the home. Privacy in the home is alive and well; it just has a new look.

Conclusion

As sensor-equipped, voice-enabled gadgets sweep through America's homes, law enforcement will be offered an unprecedented window into private residences—long considered the paragon of privacy from prying government eyes. The rise of smart home technology and the intimate data it generates and often stores on third-party servers will force courts to confront challenging, novel questions about the Fourth Amendment's reach. A conceptual view of the Court's Fourth Amendment jurisprudence reveals that the Fourth Amendment's protections evolve in response to technologies that reshape the dynamic between people and police. The smart home will be one such technology. Whatever doctrinal route courts ultimately take—relying on the sanctity of the home, assessing the privacy and surveillance threats posed by searching the smart home, or paring back the third-party doctrine—smart home technology will not tear down the walls of the Fourth Amendment home. Nor should it. While smart home devices may ultimately reduce people's control over data flows originating from within their homes, they actually intensify the refuge offered by the home. And it is the home's capacity to offer us refuge—not its ability to shield our information—that justifies so unwavering a commitment to protecting its privacy.