THE WALLS HAVE EARS . . . AND EYES . . . AND NOSES: HOME SMART DEVICES AND THE FOURTH AMENDMENT

Ryan G. Bishop*

Home. It's more than just four walls and a roof over your head. It's where you feel safest and most comfortable. But what if your home knew you as well as you know it? What if it could recognize you, and anticipate your needs? . . . What if your home became—in small ways, then big ones—an extension of you?

–Nest Website[1]

TABLE OF CONTENTS

---

* J.D. Candidate, University of Arizona James E. Rogers College of Law, Class of 2020. Thank you to Professor Jane Bambauer for her insightful feedback and help this past year, and to the editors of the *Arizona Law Review* for their diligent editing and hard work. Special thanks to my mother Lisa and my sister Rianna for their boundless support, compassion, and inspiration. This Note is dedicated to my father Geoff Bishop.

1. NEST, https://nest.com/about/ [https://web.archive.org/web/20190613222058/https://nest.com/about/].

INTRODUCTION

American homes are increasingly inhabited by "smart" devices like voice-activated speakers, robotic vacuums, and adaptive thermostats that collect, store, and share information using the Internet of Things ("IoT"). The Internet of Things refers to "an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people."[2] This interconnected environment enables devices to amass vast amounts of information about their users and glean important details about their behavior. For example, the Nest learning thermostat can connect to a user's smartphone and access its location data.[3] If the phone's location moves away from home, Nest recognizes that the user is no longer home and turns down the heat or air conditioning to save energy.[4]

Smart devices come in many different shapes and sizes and serve a wide variety of functions.[5] The Amazon Echo is a smart speaker with a digital assistant named Alexa, which listens to audio commands and can play music, make calls, and make online purchases, to name only a few functions.[6] Some devices may seem like novelties. The GeniCan is a smart trashcan that scans the barcodes of discarded products, automatically adds them to a smartphone's shopping list, and sends a text when the trashcan is full.[7] Other devices are part of a consolidated user interface that connects multiple different in-home devices. The Wink Hub is a software platform that allows a user to control any connected device, including lightbulbs, door locks, thermostats, garage doors, and water mains.[8]

The smart home market in the United States is rapidly growing and is predicted to continue this trajectory in the immediate future.[9] In 2018, Nielsen estimated that nearly a quarter of all homes in the United States owned a smart

---

2. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 1 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

3. *How Home/Away Assist Uses Your Phone's Location*, NEST, https://support.google.com/googlenest/answer/9262475?hl=en (last visited Apr. 21, 2019).

4. *Id.*

5. *See* Matthew Ashton, Note, *Debugging the Real World: Robust Criminal Prosecution in the Internet of Things*, 59 ARIZ. L. REV. 805, 807–08 (2017).

6. Taylor Martin, Tauren Dyson & David Priest, *The Complete List of Alexa Commands So Far*, CNET (Jan. 23, 2019, 12:45 PM), https://www.cnet.com/how-to/amazon-echo-the-complete-list-of-alexa-commands/.

7. GENICAN, https://www.genican.com/ (last visited Apr. 21, 2019).

8. WINK, https://www.wink.com/about/ (last visited Apr. 21, 2019).

9. Sonny Ali & Zia Yusuf, *Mapping the Smart-Home Market*, BOSTON CONSULTING GROUP 2 (Oct. 1, 2018), http://image-src.bcg.com/Images/BCG-Mapping-the-Smart-Home-Market-Oct-2018_tcm9-204487.pdf (some observers predict that between 2017 and 2022, the smart home market will achieve a compound annual growth rate of 42%.).

speaker device,[10] and Adobe predicted that almost half of American consumers would own a smart speaker by the end of 2018.[11] Altogether, the smart home market has received nearly $12 billion in investments.[12] Aside from the profitability of the devices themselves, the data collected from these devices is becoming a lucrative business opportunity. By 2020, it is estimated that transferring and disclosing IoT data will become more profitable than selling the devices themselves.[13] Alex Frommeyer, the co-founder of Beam Technologies, which sells a smart toothbrush that tracks brushing time, says that "[p]eople often refer to us as a toothbrush company, but we're not. We're actually not interested in toothbrushes at all. We're interested in health data."[14]

Law enforcement agencies are beginning to notice the potential evidentiary goldmine that home smart devices could provide for investigations.[15] One smart device company has already begun working with U.S. law enforcement agencies to access digital information collected by these devices.[16] Ring is a doorbell security camera that can record photo and video and send alerts to a user's smartphone whenever the device detects motion, or someone rings the doorbell.[17] Over 400[18]

---

10. Micah Singleton, *Nearly a Quarter of US Households Own a Smart Speaker, According to Nielsen*, THE VERGE: CIRCUIT BREAKER (Sept. 30, 2018, 10:00 AM), https://www.theverge.com/circuitbreaker/2018/9/30/17914022/smart-speaker-40-percent-us-households-nielsen-amazon-echo-google-home-apple-homepod.

11. Giselle Abramovich, *Study Finds Consumers Are Embracing Voice Services. Here's How*, CMO.COM (Sept. 10, 2018), https://www.cmo.com/features/articles/2018/9/7/adobe-2018-consumer-voice-survey.html#gs.73iq4v. To see the referenced figures, click on the slideshow at the bottom of the article; then click to the fifth slide.

12. Ali & Yusuf, *supra* note 9, at 1.

13. Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 435 (2018).

14. Kate Kaye, *There's Data in that Toothbrush (and Lots of Other Products, too)*, AD AGE (May 20, 2013), https://adage.com/article/dataworks/toothbrushes-pill-packages-record-consumer-data/241557/.

15. *See, e.g.*, Thomas Brewster, *Smart Home Surveillance: Governments Tell Google's Nest to Hand Over Data 300 Times*, FORBES (Oct. 13, 2018, 8:31 AM), https://www.forbes.com/sites/thomasbrewster/2018/10/13/smart-home-surveillance-governments-tell-googles-nest-to-hand-over-data-300-times/#80f8fee2cfa7; Todd Feathers, *Amazon Echo: Personal Assistant or Evidentiary Stronghold?*, GOV'T TECH. (Nov. 20, 2018), https://www.govtech.com/analytics/Amazon-Echo-Personal-Assistant-or-Evidentiary-Stronghold.html.

16. Caroline Haskins, *Amazon Told Police It Has Partnered with 200 Law Enforcement Agencies*, VICE: MOTHERBOARD (July 29, 2019, 10:43 AM), https://www.vice.com/en_us/article/j5wyjy/amazon-told-police-it-has-partnered-with-200-law-enforcement-agencies.

17. Matthew Guariglia, *Amazon's Ring is a Perfect Storm of Privacy Threats*, ELEC. FRONTIER FOUND. (Aug. 8, 2019), https://www.eff.org/deeplinks/2019/08/amazons-ring-perfect-storm-privacy-threats.

18. Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Reach*, WASH. POST (Aug. 28, 2019, 1:50 PM), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/.

U.S. law enforcement agencies have entered a confidential partnership with Amazon, Ring's parent company, where Amazon will donate Ring devices to an agency that in turn distributes those devices to residents.[19] Amazon then gives police access to a "Law Enforcement Neighborhood Portal," which shows police the location of all active Ring cameras in town and allows them to directly request camera footage from Ring users without a warrant.[20] In February 2019, the El Monte Police Department in California began a program where the department would reward residents who reported crime and promised to testify against suspects in court with free Ring cameras.[21] This close relationship between law enforcement and private companies endangers the Fourth Amendment's privacy protections.[22]

Police may be tempted to access data collected by other smart devices. Consider the Foobot air quality monitor, a smart device that can analyze the air in a user's home and send information about it to a user's smartphone.[23] Foobot can measure humidity and temperature, but also levels of particulate matter and chemical contaminants like formaldehyde, ammonia, and methane.[24] If the police could access this data, they could use it to investigate drug manufacturing or the use of bleach to clean up a murder scene. This data can also give insights into the behavior of people inside the home.[25] An increased level of particulates could indicate a person waking up, arriving home, or starting a fire.[26] A device normally used to inform residents about their own homes could be transformed into a government informant against them.[27]

---

19. Caroline Haskins, *Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement*, VICE: MOTHERBOARD (July 25, 2019, 8:54 AM), https://www.vice.com/en_us/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement.

20. *Id.* Under Fourth Amendment jurisprudence, police do not need a warrant to request that a person consent to a search. *See Schneckloth*, *infra* note 58. But police cannot access the sought-after information without the person's consent or a warrant. Ring owners would still have to consent to giving their footage to police.

21. Caroline Haskins, *Police Promised Witnesses Free Ring Surveillance Cameras if They Testified Against Neighbors*, VICE: MOTHERBOARD (Aug. 15, 2019, 11:13 AM), https://www.vice.com/en_us/article/kz4agn/police-promised-witnesses-free-ring-surveillance-cameras-if-they-testified-against-neighbors.

22. This Note will focus on smart devices that collect data about the interior of a home, not devices like Ring that collect information about a home's exterior. Residents still retain Fourth Amendment privacy interests in the "curtilage" immediately surrounding a home, but police still have an implicit license to approach a home's exterior for "sharply circumscribed" purposes. Florida v. Jardines, 569 U.S. 1, 6–9 (2013). For a deeper discussion of how the Fourth Amendment applies to a home's curtilage, *see generally* Carol A. Chase, *Cops, Canines, and Curtilage: What* Jardines *Teaches and What it Leaves Unanswered*, 52 HOUS. L. REV. 1289 (2015).

23. FOOBOT, https://foobot.io/features/ (last visited Apr. 18, 2019).

24. FOOBOT, https://foobot.io/foobotspecs.pdf (last visited Apr. 18, 2019).

25. *See* FOOBOT, https://foobot.io/features/ (last visited Apr. 18, 2019).

26. *Id.*

27. *See* Daniel Zwerdling, *Your Home is Your . . . Snitch?*, MARSHALL PROJECT: JUST. LAB (May 24, 2018, 12:30 PM), https://www.themarshallproject.org/2018/05/24/your-home-is-your-snitch.

The transformation of the American home spurred by smart devices necessitates the creation of new rules to bolster Fourth Amendment protections. These devices have the potential to provide a pervasive and panoptic view of a person's daily life, detailing everything from how they like their toast to the layout of their home. This massive surveillance implicates serious privacy concerns for device users. On the other hand, the data collected by these devices has the potential to greatly assist police in solving crimes and capturing criminals. To balance these competing concerns, this Note proposes a theoretical framework for assessing the level of privacy each type of smart device data merits under the Fourth Amendment.

In the past, the Supreme Court has been reluctant to "contemplate the Fourth Amendment implications of . . . frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society."[28] But over half a century later, that vaunted and frightening age is here and must be reckoned with. The Court has expressed a willingness to craft rules that "take account of more sophisticated systems that are already in use or in development."[29] As new technologies have developed such as thermal-imaging devices,[30] smartphones,[31] GPS trackers,[32] and cell phone location towers,[33] the Court has adjusted Fourth Amendment doctrine to restore the prior equilibrium.[34] The Court does not want to leave homeowners "at the mercy of advancing technology."[35]

Fourth Amendment jurisprudence is a rich and ornate area of law, and this Note will not fully examine every smart device or all the issues smart devices may present. This Note focuses on smart devices primarily used in the home because of the special importance of the home in Fourth Amendment jurisprudence.[36] Smartphones and wearable technologies, like Fitbit, certainly invoke Fourth Amendment interests, but their use outside of the home implicates different concerns.[37] It is helpful to build a Fourth Amendment framework in the hearth of the home before expanding the framework beyond the home's four walls. Lastly,

---

28. Silverman v. United States, 365 U.S. 505, 509 (1961).

29. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)). The Court acknowledged that its holding is based on the state of cell-site location information ("CSLI") technology in the early 2010s. But it also recognized that CSLI is quickly becoming as precise as Global Positioning System ("GPS") data. The Court predicted that the continued proliferation of smartphones will enable an even greater ability to precisely estimate a phone's location from CSLI.

30. *Kyllo*, 533 U.S. at 29.

31. Riley v. California, 573 U.S. 373, 378–79 (2014).

32. United States v. Jones, 565 U.S. 400, 402 (2012).

33. *Carpenter*, 138 S. Ct. at 2211.

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

35. *Kyllo*, 533 U.S. at 35–36.

36. *See* Florida v. Jardines, 569 U.S. 1, 6 (2013) ("But when it comes to the Fourth Amendment, the home is first among equals."); Agnello v. United States, 269 U.S. 20, 32 (1925) ("The search of a private dwelling without a warrant is in itself unreasonable and abhorrent to our laws.").

37. *See* Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 590–91 (2017).

this Note will focus on smart devices used in residential structures, but it is important to remember that smart devices are increasingly being used in other buildings like offices,[38] warehouses,[39] hospitals,[40] museums,[41] and schools.[42] A person may have a diminished expectation of privacy in these areas.[43]

Part I will lay out the basics of Fourth Amendment law and how courts approach questions of privacy and searches. This Part will also explore some warrant exception categories, and how they might apply to searches of smart device data. Part II will focus on the third-party doctrine, and how recent developments may inform the way courts will assess data gathered by smart devices going forward. Part III will lay out a new framework for analyzing the relative protections of different data types under the Fourth Amendment.

I. SUMMARY OF FOURTH AMENDMENT DOCTRINE

A. The Property-Based Approach and the Katz *Test*

The Fourth Amendment declares, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[44] To secure against these unreasonable searches and seizures, "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[45] The first task in interpreting this Amendment is to define what a "search" is because unless a search or seizure is involved the Amendment's protections are not invoked.

---

38. Steve Ranger, *IoT in the Office: Everything You Need to Know About the Internet of Things in the Workplace*, ZDNET (Mar. 28, 2018, 3:00 AM), https://www.zdnet.com/article/iot-in-the-office-everything-you-need-to-know-about-the-internet-of-things-in-the-office/.

39. Noel McKeon, *How the IoT Can Help Create Smart Warehouses*, INTELLITRACK (Nov. 12, 2017), https://www.intellitrack.net/iot-can-help-create-smart-warehouses/.

40. Cadie Thompson, *As Healthcare Costs Rise and Patients Demand Better Care, Hospitals Turn to New Technologies*, BUS. INSIDER (Oct. 26, 2016, 8:22 PM), https://www.businessinsider.com/how-hospitals-are-using-iot-2016-10.

41. Rebecca Hiscott, *United Nations Simulates Violent Land Mines via Apple iBeacons*, MASHABLE (Apr. 4, 2014), https://mashable.com/2014/04/04/ibeacons-land-mines-simulation/.

42. Frederic Paul, *The Internet of Things Goes to School*, NETWORKWORLD: TECHWATCH (Aug. 30, 2017, 8:19 AM), https://www.networkworld.com/article/3221126/internet-of-things/the-internet-of-things-goes-to-school.html.

43. *See* O'Connor v. Ortega, 480 U.S. 709, 718 (1987) ("Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis."). For example, the Court ruled that it was reasonable under the Fourth Amendment for an employer to review the pager transcripts of an employee who sent sexually-explicit messages to a work pager and knew of a policy granting his employer the right to monitor and log all pager activity. City of Ontario v. Quon, 560 U.S. 746, 752–53, 764–65 (2010).

44. U.S. CONST. amend. IV.

45. *Id.*

The Court may take two major routes to determine whether a Fourth Amendment search occurred: (1) the property-based approach and (2) the reasonable expectation of privacy approach (also known as the *Katz*[46] test). The property-based approach emphasizes the historical reverence of property rights in the colonial era leading up to the American Revolution.[47] The Court encourages starting any search analysis with the property-based approach as a baseline because it "keeps easy cases easy."[48] But the property-based approach to searches is the floor of the Fourth Amendment, not the ceiling.[49] Even if no physical trespass onto a person's property occurs, a search occurs when an officer invades an area where one has a reasonable expectation of privacy.[50] The person must have a subjective expectation of privacy in that area, and the expectation must be one society is prepared to recognize as reasonable.[51]

B. Non-Searches and Warrant Exception Categories

The Court has recognized several categories of information collection by police that are not searches and thus do not require a warrant. First is the plain- view doctrine, which states that "if an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy."[52] The rule for plain-view seizure states that an officer must be able to view the article from a lawful vantage point, the officer must have a lawful right to access the article itself, and the incriminating character of the article must be immediately apparent.[53] Most data collected by smart devices will not be in "plain view" as it has been commonly understood. For example, the raw data from a smart air quality monitor likely cannot

---

46. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

47. *See* United States v. Jones, 565 U.S. 400, 404–05 (2012) (quoting Entick v. Carrington, 95 Eng. Rep. 807, 817 (C.P. 1765)) ("[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, [. . .] if he will tread upon his neighbour's ground, he must justify it by law."); Payton v. New York, 445 U.S. 573, 583 (1980) ("It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment.").

48. *See* Florida v. Jardines, 569 U.S. 1, 6, 11 (2013).

49. *See, e.g.*, *Jones*, 565 U.S. at 409 ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test."); Soldal v. Cook Cty., 506 U.S. 56, 64 (1992) ("[P]roperty rights are not the sole measure of Fourth Amendment violations."); Silverman v. United States, 365 U.S. 505, 511 (1961) ("Inherent Fourth Amendment rights are not inevitably measurable in terms of ancient niceties of tort or real property law.").

50. *See Katz*, 389 U.S. at 360–61 (Harlan, J., concurring).

51. *Id.* at 361. This approach has been criticized for being based on "judicial speculation" and not statistical evidence of what society's actual privacy expectations are. Bernard Chao, Catherine Durso, Ian Farrell & Christopher Robertson, *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CALIF. L. REV. 263, 319 (2018). The authors of this study surveyed a sample of 1,200 participants and asked them to assess the reasonableness of 18 different investigative actions. *Id.* at 294. The survey results do not match judicial findings of when *Katz* is triggered. *Id.* at 308, tbl.4.

52. Horton v. California, 496 U.S. 128, 133 (1990).

53. *Id.* at 136–37.

be viewed or accessed from a lawful vantage point, and the incriminating nature would likely not be immediately apparent.[54] The relevant non-search rules for smart devices come from cases interpreting the third-party doctrine. This line of cases holds that evidence voluntarily disclosed to a third party is not private, and thus a police officer's access to that evidence is not a search.[55] But as discussed in Part II, the Court has been narrowing the scope of the third-party doctrine.[56]

The Court also recognizes categories of information collection that are searches but are justifiable without the need for a warrant.[57] If a person voluntarily consents to a search by police, the search is reasonable and does not require a warrant.[58] If the police ask a person to allow a search of a Roomba vacuum's data, and the person obliges absent any coercion,[59] the search is reasonable. However, the boundaries of consent and what qualifies as a voluntary disclosure in the context of digital data are not yet fully set.[60]

---

54. But certain devices can share the data they collect publicly on social media and thus may implicate the plain-view doctrine. Ring doorbell camera users can connect their Ring device to social media networks and post videos recorded by their devices. Todd Haselton, *Everyone's Talking About this Amazon App that Lets Police See Camera Footage – Here's What It's Like*, CNBC (Aug. 3, 2019, 9:30 AM), https://www.cnbc.com/2019/08/02/amazon-ring-neighbors-app-sends-video-to-police-departments.html. Assuming the post is public and the footage's incriminating nature is immediately apparent, an officer viewing the footage would be at a constitutional vantage point, and it would not be a search.

55. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

56. *See infra* Part II.

57. Other categories of warrant exceptions exist beyond the ones mentioned above. These include sobriety checkpoints (Michigan Dep't of State Police v. Sitz, 496 U.S. 444, 447 (1990)), searches of automobiles (California v. Carney, 471 U.S. 386, 390 (1985)), and stop-and-frisk searches (Terry v. Ohio, 392 U.S. 1, 9–10 (1968)). This Note will not discuss these exceptions because they all occur outside of the home. The question of which Fourth Amendment concerns arise from police searches of smart devices on one's person or in one's car is ripe for further research.

58. Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

59. *Id.* at 227 ("While knowledge of the right to refuse consent is one factor to be taken into account, the government need not establish such knowledge as the sine qua non of an effective consent.").

60. The FBI has been paying members of Best Buy's Geek Squad, an electronic product repair service, as informants to search the content of computers turned over by customers for repair. Now, a California man faces federal charges for possession of child pornography found on his hard drive by Geek Squad informants. *See* Orin Kerr, *The Geek Squad and the Fourth Amendment*, WASH. POST: VOLOKH CONSPIRACY (Jan. 11, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/01/11/the-geek-squad-and-the-fourth-amendment/?utm_term=.214bfaa5f3f0. This raises several questions about consent: did the suspect waive consent by relinquishing his computer over to the Geek Squad for repair? Do Geek Squad employees have independent authority to consent to a government search? Did the informant's examination exceed the scope of the suspect's consent? The last question is especially interesting because the pornographic images were found in a space on his hard drive accessible only by specialized forensic tools. *See* R. Scott Moxley, *Best Buy Geek Squad Informant Use Has FBI on Defense in Child-Porn Case*, OC WKLY. (Jan. 4,

Another kind of justifiable search is a search incident to a lawful arrest.[61] When an officer arrests someone, it is reasonable for that officer to search the arrestee's person and the area within the arrestee's immediate control.[62] This exception is grounded in the need to ensure the arresting officer's safety from any weapons the arrestee may have immediate access to and the need to preserve evidence from destruction.[63] In *Riley v. California*, the Court found that police could not search cell phone data under this exception because neither justification applied.[64] First, the Court recognized the obvious fact that "digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape."[65] Second, it found that the destruction of data on the phone was theoretically possible using remote wiping or data encryption, but that these concerns were too remote to justify a blanket rule authorizing a warrantless search of digital records during an arrest.[66]

Just as the Court in *Riley* found these justifications unpersuasive as applied to cell phone data, an arrest of someone in their home would likely not justify a warrantless search of the smart devices in their immediate control. A Roomba, Nest, or Google Home presents no threat to officer safety that justifies accessing the device's digital data. The likelihood that important digital data will be destroyed unless officers access those devices at the time of arrest is improbable.[67] As the Court noted in *Riley*, options like a Faraday bag (an aluminum foil bag which isolates a phone from radio waves that may trigger a remote wipe of the device's

---

2017), https://ocweekly.com/best-buy-geek-squad-informant-use-has-fbi-on-defense-in-child-porn-case-7794252/.

61. It is also reasonable for police officers to perform a protective sweep of a home while arresting someone to assure officer safety from possible hidden attackers. But, the scope of the sweep is limited only to "a cursory inspection of those spaces where a person may be found," and must last "no longer than is necessary to dispel the reasonable suspicion of danger." Maryland v. Buie, 494 U.S. 325, 335–36 (1990). A protective sweep would not permit an officer to examine a device's stored data, because a person obviously cannot hide in a device's digital files.

62. Chimel v. California, 395 U.S. 752, 762–63 (1969).

63. *Id.*

64. Riley v. California, 573 U.S. 373, 386, 388 (2014).

65. *Id.* at 387.

66. *Id.* at 388–90. *But see* Steven Cook, *Suspect in Remote Phone-Wiping Case Denies Wrongdoing*, DAILY GAZETTE (Nov. 12, 2018), https://dailygazette.com/article/2018/11/12/suspect-in-remote-phone-wiping-case-denies-wrongdoing.

67. This is not to say that every home smart device shares the same evidence destruction possibilities as the smartphones at issue in *Riley*. One can imagine a situation where an arrestee has programmed their Google Home to delete incriminating stored information upon a voice command. This may justify removing the arrestee from the device's hearing range, or even powering off the device to prevent such a data wipe. The Court has never found unlawful a "temporary seizure that was supported by probable cause and was designed to prevent the loss of evidence while the police diligently obtained a warrant in a reasonable period of time." Illinois v. McArthur, 531 U.S. 326, 334 (2001).

data) are available to police and seem to be a less restrictive alternative to searching the smart device on the spot.[68]

Administrative searches are a type of justifiable warrantless search particularly relevant to some smart devices like utility meters. An administrative search is a search conducted in pursuit of a regulatory or safety goal unrelated to criminal law enforcement.[69] These include searches of residential[70] and commercial[71] buildings, or searches of closely regulated industries.[72]

The Fourth Amendment's warrant requirement has an exigency exception. Warrantless searches are presumptively unreasonable "unless 'the exigencies of the situation' make the needs of law enforcement so compelling that the warrantless search is objectively reasonable under the Fourth Amendment."[73] Exigencies that might warrant intruding on private property include fighting a fire, preventing the imminent destruction of evidence, engaging a fleeing suspect in hot pursuit, or breaking up a fight.[74] Many exigency cases concern an officer physically entering a person's home, not accessing digitally-stored information.[75]

II. THE THIRD-PARTY DOCTRINE

A. The Doctrine in Smith *and* Miller

The third-party doctrine grew out of *Katz's* reasonable expectation of privacy approach. The doctrine states that a person has no legitimate expectation of privacy in information they voluntarily turn over to third parties.[76] If a person has no legitimate expectation of privacy in such information, then the police may conduct a warrantless search of that information without offending the Constitution.[77] In *Smith v. Maryland*, the Court held that a man who made threatening and obscene calls to a robbery witness had no reasonable expectation of privacy in his phone number because he voluntarily disclosed it to the phone company.[78] The Court held that the defendant did not have a reasonable subjective expectation of privacy in his phone number because it is unreasonable to expect that a phone company would not make a permanent record of phone numbers dialed by

---

68. *Riley*, 573 U.S. at 390–91.

69. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000) ("[W]e decline to approve a program whose primary purpose is ultimately indistinguishable from the general interest in crime control.").

70. Camara v. Mun. Court of S.F., 387 U.S. 523, 528–29 (1967).

71. Donovan v. Dewey, 452 U.S. 594, 598–99 (1981).

72. New York v. Burger, 482 U.S. 691, 702 (1987) (holding statutorily authorized warrantless inspections of vehicle junkyards were reasonable under the Fourth Amendment because the long history of government oversight over junkyards obviated the owner's reasonable expectation of privacy).

73. Mincey v. Arizona, 437 U.S. 385, 393–94 (1978).

74. Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

75. *See generally* Kentucky v. King, 563 U.S. 452, 455 (2011); *Brigham City*, 547 U.S. at 400; Warden v. Hayden, 387 U.S. 294, 296–97 (1967).

76. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

77. *Id.* at 745–46.

78. *Id.* at 737, 744–45.

customers.[79] For the second, objective prong of the *Katz* analysis, the Court found that society is not prepared to recognize a claim of privacy in phone numbers.[80] Even if a defendant claims to have a subjective expectation of privacy in their number, this expectation is objectively "illegitimate" in the eyes of society.[81]

In *United States v. Miller*, the Court ruled that a defendant suspected of fraud had no reasonable expectation of privacy in his bank records.[82] The Court held that the checks voluntarily disclosed to the bank by the defendant were not "confidential communications, but negotiable instruments to be used in commercial transactions."[83] The Court in *Smith* and *Miller* placed importance on the risk that the third party could convey the information to the government.[84] The general public knowledge that phone companies and banks require disclosure of certain kinds of information undercuts one's expectation that the information conveyed will remain secret and protected from the eyes of the government.[85] This social understanding gives citizens a degree of notice that removes the surprise that occurs when police obtain their personal information.

Miller seems to imply that information used for a commercial purpose, like a check delivered to a bank, merits weakened Fourth Amendment protections. But how does this inference translate to the business models of most prominent technology companies today? As the popular modern adage goes, "[y]ou're not Facebook's customer. You're Facebook's product."[86] Smart device data collected by consumer products necessarily has a commercial nature like the checks and deposit slips in *Miller* did. If information about a person's interests, voice, appearance, or coffee preferences has a commercial nature, does this undermine an individual's privacy interests in that information? The Court ought to reconsider this aspect of *Miller* in light of today's economic environment, which is influenced heavily by the harvesting of consumer data.

---

79. *Id.* at 742–43.

80. *Id.* at 743–44.

81. *Id.* at 745.

82. United States v. Miller, 425 U.S. 435, 442 (1976).

83. *Id.*

84. *See Smith*, 442 U.S. at 745 ("In these circumstances, petitioner assumed the risk that the information would be divulged to the police."); *Miller*, 425 U.S. at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971)) ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").

85. *Smith*, 442 U.S. at 743 ("Telephone users, in sum, typically know that they must convey numerical information to the phone company . . . ."). *Contra id.* at 749 (Marshall, J., dissenting) ("[I]t does not follow that [individuals] expect this information to be made available to the public in general or the government in particular.").

86. Edward Morrissey, *You're Not Facebook's Customer. You're Facebook's Product*, THE WEEK (Mar. 21, 2018), https://theweek.com/articles/761830/youre-not-facebooks-customer-youre-facebooks-product. *Cf.* Will Oremus, *Are You Really the Product?*, SLATE (Apr. 27, 2018, 5:55 AM), https://slate.com/technology/2018/04/are-you-really-facebooks-product-the-history-of-a-dangerous-idea.html.

B. The Doctrine After Carpenter

In 2018, the Court narrowed the third-party doctrine in *Carpenter v. United States*, a "blockbuster"[87] ruling for the Fourth Amendment.[88] This case concerned two orders issued under the Stored Communications Act for suspected robber Timothy Carpenter's cell-site location information ("CSLI") from two wireless service providers.[89] The orders sought 152 days of CSLI records from MetroPCS and 7 days from Sprint, of which 127 days and 2 days were produced, respectively.[90] CSLI is a time-stamped record logged whenever a cell phone connects to a cell site which is collected and stored by wireless carriers.[91] The CSLI from his phone was used to place him at the scene of several robberies, and he was convicted as a result.[92]

In determining whether the government's retrieval of CSLI was a search, the Court had to reconcile the new phenomenon of location data, which is continually chronicled by wireless providers, with the structure of *Smith* and *Miller*. The Court decided not to extend *Smith* and *Miller* to the "unique" nature of CSLI and declared that "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[93] Today, smartphones are practically a "feature of human anatomy," and the encyclopedic cataloging of location data allows an unrestrained government to "achieve[] near perfect surveillance."[94] Following *United States v. Jones*, which held that attaching a GPS device to a car to track its movements is a search, the Court reasoned that "individuals have a reasonable expectation of privacy in the whole of their physical movements."[95] The Court held that both the defendant and society at large are prepared to recognize a reasonable expectation of privacy in CSLI as legitimate.[96] By recognizing a privacy interest in CSLI, the Court set a new path for certain types of data to achieve Fourth Amendment protection despite being held by third parties:

> There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to *a distinct category of information*.[97]

---

87. ORIN KERR, *Implementing* Carpenter, *in* THE DIGITAL FOURTH AMENDMENT (forthcoming) (manuscript at 1) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257.

88. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

89. *Id.* at 2212.

90. *Id.*

91. *Id.* at 2211–12.

92. *Id.* at 2212–13.

93. *Id.* at 2217.

94. *Id.* at 2218 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

95. *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 430 (2012)).

96. *Id.* The Court declined to set a definitive benchmark for the number of days' worth of CSLI data that would trigger Fourth Amendment protection. The Court held only that accessing seven days or more worth of CSLI requires a warrant. *Id.* n.3.

97. *Id.* at 2219 (emphasis added).

What does this standard mean for the third-party doctrine going forward? The Court in *Carpenter* did not try to address all possible future applications of the doctrine and focused only on CSLI records.[98] As Justice Gorsuch questioned in dissent, "how are lower courts supposed to weigh these radically different interests, or assign values to different categories of information?"[99] Part III will address Justice Gorsuch's concerns and provide a durable framework for assessing whether new categories of information escape the third-party doctrine or whether they remain outside of the Fourth Amendment's warrant protections.[100]

While Justice Gorsuch characterizes *Smith* and *Miller* as "on life support,"[101] the Court does not yet seem ready to abandon those cases entirely.[102] These cases may just be quarantined to situations where a reasonable person has robust knowledge of what data that person is actually disclosing. Mr. Smith must have known that his phone number was bound to be disclosed, and Mr. Miller must have known that the bank could read his checks at any time. But how much does a person reasonably know about what information their smart speaker collects?[103]

Another way to distinguish the third-party doctrine's application in *Miller* and *Smith* from *Carpenter* is to consider how the disclosure of information occurs. In *Miller*, the defendant actively deposited his checks at the bank, and in *Smith*, the defendant actively dialed his target's phone number to establish a call and threaten her.[104] By contrast, the CSLI in *Carpenter* was harvested without any action of the smartphone user beyond merely possessing the phone.[105] The data is collected by virtue of the phone's sheer existence on the network.[106] Many home smart devices

---

98. *Id.* at 2220.

99. *Id.* at 2267 (Gorsuch, J., dissenting).

100. *See infra* Part III.

101. *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).

102. *Id.* at 2220 (majority opinion). ("We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras.").

103. *See* Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, BUS. INSIDER (Nov. 15, 2017, 7:30 AM), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 ("A Deloitte survey of 2,000 consumers in the U.S found that 91% of people consent to legal terms and services conditions without reading them. For younger people, ages 18-34 the rate is even higher with 97% agreeing to conditions before reading."). A recent study found that 99% of the terms of service for 500 popular websites "required at least 14 years of education to truly comprehend." Cory Doctorow, *Most Adults Are Incapable of Understanding Most Online Terms of Service*, BOINGBOING (Feb. 14, 2019, 10:04 AM), https://boingboing.net/2019/02/14/i-agree-to-disagree.html.

104. United States v. Miller, 425 U.S. 435, 437–38 (1976); Smith v. Maryland, 442 U.S. 735, 737 (1979).

105. *Carpenter*, 138 S. Ct. at 2220 ("[I]n no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements." (quoting *Smith*, 442 U.S. at 745)).

106. *Id.*

already work off of the same kind of passive data collection that smartphones do.[107] The smart device market is trending toward the ubiquity of devices that are always on and always collecting information.[108]

One could argue that even if smart devices operate passively, the user still initiated data collection by setting up the device in the first place. Even though a Roomba vacuum collects information on its own,[109] a user still initially set up the Roomba and enabled it to collect the information. The difficulty with this argument is that it would allow police to search the data of any commercial product without a warrant because a voluntary assumption of risk[110] could always be traced back to the product's purchase.[111] This argument is especially unpersuasive considering products like smartphones are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[112]

If smartphones are pervasive and necessary, what about smart devices? One could argue that some smart devices, like smart toasters[113] and remote pet food dispensers,[114] are luxuries, not daily necessities. But in some situations, the use of a home smart device is required, like a government-mandated smart utility meter.[115]

---

107. The Piper home security system has a camera and motion sensors that automatically detect and record movement inside the home. *See How It Works*, PIPER, https://getpiper.com/howitworks/ (last visited Apr. 21, 2019).

108. Christopher Mims, *All Ears: Always-On Listening Devices Could Soon Be Everywhere*, WALL STREET J. (July 12, 2018, 12:00 PM), https://www.wsj.com/articles/all-ears-always-on-listening-devices-could-soon-be-everywhere-1531411250.

109. Evan Ackerman & Erico Guizzo, *iRobot Brings Visual Mapping and Navigation to the Roomba 980*, IEEE SPECTRUM (Sept. 16, 2015, 8:30 PM), https://spectrum.ieee.org/automaton/robotics/home-robots/irobot-brings-visual-mapping-and-navigation-to-the-roomba-980.

110. *Smith*, 442 U.S. at 745.

111. Professor Jameson Wetmore analogizes the invitation of a robotic vacuum into the home to the mythological rule that a vampire may not enter a home unless invited in by the owner. Jameson Wetmore, *What Can We Learn About Vacuum Cleaners from Vampires?*, IEEE CONSUMER ELECTRONICS. MAG. 103 (Feb. 8, 2018), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8287046. The mere act of "inviting" a smart vacuum into the home could constitute a waiver of Fourth Amendment rights. But the Court seems to disfavor this approach, at least with respect to smartphones, because of their ubiquity and necessity in daily life.

112. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (quoting Riley v. California, 573 U.S. 373, 385 (2014)). The Court in *Carpenter* seems to have adopted part of Justice Brennan's dissent in *Miller*, which argued that participation in "the economic life of contemporary society" is impossible without a bank account. United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting) (quoting Burrows v. Superior Court, 529 P.2d 590, 596 (Cal. 1974)).

113. Roberto Baldwin, *The World Now Has a Smart Toaster*, ENGADGET (Jan. 4, 2017), https://www.engadget.com/2017/01/04/griffin-connects-your-toast-to-your-phone/.

114. FURBO, https://shopus.furbo.com/ (last visited Apr. 21, 2019).

115. *See* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 523 (7th Cir. 2018). As a personal anecdote, the property owner of my apartment is considering saving energy costs by installing occupancy sensors, which detect whether a person is home and shut off lights and air conditioning if no one is. Although he did not

Further, the Court may be unwilling to make specific declarations about which pieces of commercial technology are necessities and which are not.[116] The Court would probably not want to tell new parents that a smart baby monitor[117] is not a necessity, that a dementia patient does not require the use of a smart pill bottle,[118] or that consumers must choose between a lower energy bill and their cherished Fourth Amendment rights.[119]

C. Smart Utility Meter Searches in Naperville

Courts have not had many chances to directly address how the Fourth Amendment applies to data from home smart devices post-*Carpenter*. But two months after *Carpenter* was decided, the Seventh Circuit analyzed Fourth Amendment protections for smart utility meter data in *Naperville Smart Meter Awareness v. City of Naperville*.[120] This case involved a suit brought by Naperville Smart Meter Awareness ("NSMA"), a group of citizens who oppose the City of Naperville's installation of digital smart energy meters on their homes.[121] These smart meters record the energy consumption of a home every 15 minutes and send that information to the City's public utility, where it is stored for up to 3 years.[122] The energy consumption readings reveal more than just the bare wattage of energy consumption because certain appliances produce specific "load signatures" that one can analyze to predict which appliances a person has in their home.[123] NSMA argued

---

specify, these could be IoT-enabled occupancy sensors. Eventually, smart devices used to limit utility usage could become standard in new homes and apartments, even if not explicitly mandated by the government. *See also* Rich Smith, *The Latest Trend in Apartment Living Hits Seattle: Forced Installation of "Smart" Devices*, THE STRANGER: SLOG (Sept. 9, 2019, 2:21 PM), https://www.thestranger.com/slog/2019/09/09/41335556/the-latest-trend-in-apartment-living-hits-seattle-forced-installation-of-smart-devices.

116. *See Carpenter*, 138 S. Ct. at 2220 (quoting Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)) ("We do not express a view on matters not before us . . . the Court must tread carefully in such cases, to ensure that we do not 'embarrass the future.'").

117. NANIT, https://www.nanit.com/ (last visited Apr. 21, 2019).

118. *How It Works*, ADHERETECH, https://www.adheretech.com/how-it-works (last visited Aug. 5, 2019).

119. *See* Michael Price & Bill Wolf, *Building on* Carpenter*: Six New Fourth Amendment Challenges Every Defense Lawyer Should Consider*, THE CHAMPION 20, 24, (Dec. 2018), https://www.nacdl.org/getattachment/c7c23b60-937f-4edd-bec4-b8e7b50ea90d/price-building-on-carpenter.pdf.

120. *Naperville*, 900 F.3d at 521.

121. *Id.* at 524. Not all smart utility meters are government-mandated. The Streamlabs Smart Water Meter records hourly water usage data and detects leaks. STREAMLABS, https://streamlabswater.com/ (last visited Apr. 21, 2019). The Sense Home Energy Monitor records real time and historical energy usage in a home, and allows users with solar panels to track energy production. *Getting Started with the Sense App*, SENSE (July 14, 2017), https://blog.sense.com/articles/getting-started-sense-app-walkthrough/.

122. *Naperville*, 900 F.3d at 524.

123. In other words, an analyst interpreting a raw energy consumption reading would be able to predict the presence of a refrigerator, television, or marijuana grow light by comparing the sample reading to a large library of appliance load signatures. *Id.*

these readings reveal "intimate details of the City's electric customers,"[124] and thus the collection of this data by the City is an unreasonable search which violates the Fourth Amendment and the Illinois Constitution.[125]

The Seventh Circuit agreed with NSMA that the data collection at 15-minute intervals was a search,[126] but held that the search was ultimately a reasonable one that did not require a warrant.[127] Relying on *Kyllo v. United States*,[128] the court found that these smart meters were not in general public use[129] and were used to explore the details of a home which were previously unknowable without physical intrusion.[130] The court found Naperville's smart meters even more invasive than the thermal imagers at issue in *Kyllo*, which were much cruder in comparison.[131] However, the court held that the City's data collection was an administrative search that did not require a warrant.[132] The government's substantial interest in gathering data from smart meters outweighed consumer privacy interests in those readings.[133] Unlike *Camara v. Municipal Court of San Francisco*, which involved the physical entry into and inspection of dwellings, a meter reading is not as intrusive and is less likely to produce a criminal prosecution.[134]

Legislative solutions may soon address the Seventh Circuit's decision. In 2017, Senator Ron Wyden of Oregon proposed a trio of bills focused on upgrading

---

124. *Id.* ("[S]uch as when people are home and when the home is vacant, sleeping routines, eating routines, specific appliance types in the home and when used, and charging data for plug-in vehicles that can be used to identify travel routines and history.").

125. *Id.*

126. Additionally, the court found that the third-party doctrine did not apply in this case. The meter data goes directly to the city-owned public utility, so no third party exists between a Naperville resident and the government. Even if one existed, the court, relying on *Carpenter*, ruled that "a home occupant does not assume the risk of near constant monitoring by choosing to have electricity in her home." *Id.* at 527.

127. *Id.* at 529.

128. Kyllo v. United States, 533 U.S. 27, 34 (2001). This case concerned the use of thermal-imaging devices by police to detect whether the defendant's house was emitting an abnormal amount of heat, indicating that marijuana was being grown inside. The Court ruled that the use of the device to reveal information about the inside of the home was a search which required a warrant. *Id.* at 40.

129. The court ruled that smart meters have only been adopted in a small fraction of cities and are not yet so pervasive in residential life as to obviate *Kyllo*. *Naperville*, 900 F.3d at 526–27. But the court also notes a lack of guidance from the Supreme Court on what the contours of "general public use" are. *Id.* This prong of *Kyllo* may have to be re-evaluated amidst the increasing prevalence of home smart devices, which are designed to be in general public use. *See* Katie Barlow, *Thermal Imaging Gets More Common but the Courts Haven't Caught Up*, NPR (Feb. 27, 2014, 12:43 PM), https://www.npr.org/sections/alltechconsidered/2014/02/25/282523377/thermal-imaging-gets-more-common-but-the-courts-havent-caught-up.

130. *Naperville*, 900 F.3d at 526.

131. *See id.*

132. *Id.* at 528–29.

133. *Id.*

134. *Compare* Camara v. Mun. Court of S.F., 387 U.S. 523, 525–26 (1967), *with Naperville*, 900 F.3d at 528.

electrical grids, encouraging the use of renewable energy, and creating grants for consumer-level solar panels.[135] Each bill contains language requiring a warrant based on probable cause for any governmental entity to access "information regarding the use of electricity by an electric consumer (including monthly usage data, data at a greater level of detail or specificity, and information about electric use by specific appliances)."[136] If passed, these provisions would give statutory privacy protections to utility data. But until then, courts may follow the Seventh Circuit's approach in *Naperville* and hold that government-mandated utility data is subject to the Fourth Amendment's administrative search exception.[137]

III. DATA-TYPE ANALYSIS

A. The Need for a New Approach

Given the rise of smart devices and the dearth of case law directly addressing them, courts will soon need to address the use of these devices in police investigations and determine the appropriate application of existing case law. *Carpenter*, which disfavors the government's ability to claim "a significant extension of [the third-party doctrine] to a distinct category of information," provides a workable path forward.[138] How should courts assess these categories of information? Smart devices collect many different kinds of data: temperature, location, audio, video, air quality measurements, and utility use, to name a few.[139] Proponents of the third-party doctrine argue diluting the doctrine will hamstring the ability of police to investigate crimes because smart devices have the potential to greatly assist police while not seriously infringing privacy.[140] Privacy advocates argue that the parameters of the third-party doctrine need to be reset in the digital age because choosing to participate in modern society requires the use of smart

---

135. Tim Cushing, *Three Energy Bills Look to Increase Fourth Amendment Protections for Americans*, TECHDIRT (Oct. 10, 2017, 7:55 PM), https://www.techdirt.com/articles/20171001/14020938328/three-energy-bills-look-to-increase-fourth-amendment-protections-americans.shtml.

136. *Id.*

137. In 2017, Minneapolis police subpoenaed the electricity-usage records of a woman suspected of growing marijuana from utility provider Xcel Energy. State v. Sparks, No. 27-CR-17-16660, 2019 WL 1890295, at *1 (Minn. Ct. App. Apr. 29, 2019). Police also obtained records of three neighboring homes to compare against the suspect's usage. *Id.* Police used the high energy-usage readings to obtain a search warrant for the suspect's home, which revealed paraphernalia and 32 marijuana plants. *Id.* On appeal, the court declined to review the constitutionality of the search of her energy records because she was convicted before *Carpenter* and *Naperville* were decided. *Id.* at *1–2.

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

139. The Nest Cam alone collects audio, video, photo, temperature, ambient light, location, and facial recognition data. *See Privacy Statement for Nest Products and Services*, NEST, https://nest.com/uk/legal/privacy-statement-for-nest-products-and-services/ (last visited Apr. 21, 2019).

140. *See Carpenter*, 138 S. Ct. at 2256 (Alito, J., dissenting) ("Many investigations will sputter out at the start, and a host of criminals will be able to evade law enforcement's reach."); Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 1048 (2016).

technologies.[141] Should the doctrine expose all smart device data to warrantless search, or none?

Creating such a bright-line rule is unnecessary to protect privacy rights without unduly hampering the ability of police to investigate crimes. To solve this, courts should adopt a data-type-based approach to Fourth Amendment protection when analyzing searches of smart devices. Courts should take a case-by-case approach to determine the relative privacy interests a smart device user has in a particular type of data—location data, audio recordings, air quality measurements, etc. Home smart devices are not all created equal—they vary wildly in their data collection capabilities. A doctrine that encompasses every device from smart sprinkler systems to smart lightbulbs to smart dolls in a way that recognizes the vastly different consequences each device has on a user's privacy interests would be difficult to create. Instead of looking at *devices*, courts should focus instead on the *types of information* collected by the devices themselves. The major question that courts should consider is: Is this particular type of data capable of revealing intimate details about a person's home that are susceptible to government abuse? If so, that type of data should not fall under the third-party doctrine and should be protected from warrantless search by the Fourth Amendment.

This will be a case-by-case approach, analogous to the selective incorporation of the Bill of Rights through the Fourteenth Amendment's Due Process Clause. In the incorporation context, the Court has not expanded the Bill of Rights to the states wholesale.[142] Instead, it has opted for a case-by-case inquiry into whether the particular protection has been "found to be implicit in the concept of ordered liberty."[143] Similarly, courts should determine whether a given data type would be implicit in the concept of ordered *privacy*, and thus inherently implicates a person's Fourth Amendment privacy interests.

This Note does not suggest that courts should arrive at a particular hierarchy of data privacy. It is not necessarily true that, given all the data types that may exist, there should be a normal distribution of privacy interests, with 50% warranting Fourth Amendment protection and 50% not warranting protection. Perhaps, after examining the relative privacy interests of 100 data types, the Court determines 99 are worthy of Fourth Amendment protection and 1 is not. In terms of a hierarchy, a court may judge location data to be relatively more intimate than

---

141. *See* Jennifer Lynch, *Symposium: Will the Fourth Amendment Protect 21st-Century Data? The Court Confronts the Third-Party Doctrine*, SCOTUSBLOG (Aug. 2, 2017, 12:21 PM), https://www.scotusblog.com/2017/08/symposium-will-fourth-amendment-protect-21st-century-data-court-confronts-third-party-doctrine/.

142. Although the majority of the Bill of Rights has been incorporated to the states, the Third Amendment, the Seventh Amendment, and the Fifth Amendment's Grand Jury Clause have not yet been incorporated. Lana Ulrich, *Should the Excessive Fines Clause Apply Against the States?*, NAT'L CONST. CTR. (Sept. 5, 2018), https://constitutioncenter.org/blog/should-the-excessive-fines-clause-apply-against-the-states. In 2019, the Court incorporated the Eighth Amendment's protection against excessive fines to the states. Timbs v. Indiana, 139 S. Ct. 682, 687 (2019).

143. Palko v. Connecticut, 302 U.S. 319, 324–25 (1937).

utility usage data, but still find both are sufficiently worthy of constitutional protection.

This sort of spectrum approach is not foreign to the courts. Courts utilize a spectrum approach for cases involving the First Amendment freedom of intimate association.[144] In these cases, courts must decide whether a law violates a person's right to join a group and associate with others.[145] But the First Amendment's protections only extend to certain categories of relationships.[146] In *Roberts v. U.S. Jaycees*, the Court ruled that "[d]etermining the limits of state authority over an individual's freedom to enter into a particular association therefore unavoidably entails a careful assessment of where that relationship's objective characteristics locate it on a spectrum from the most intimate to the most attenuated of personal attachments."[147] If courts feel comfortable applying a spectrum approach to sort out what counts as an intimate human relationship, it does not seem farfetched to apply this same logic to smart device data. Courts should assess the objective characteristics of data collected by a device to locate those data types on a spectrum from the most intimate to the most attenuated of privacy concerns.

B. The Device-Based Approach

This Note argues that a data-centered approach is preferable to a device-centered approach. Professor Orin Kerr proposes a new approach to the third-party doctrine in the wake of *Carpenter*.[148] Kerr suggests a three-pronged test that applies *Carpenter* to a search of Internet records if such records exist because of the digital age, are created without meaningful voluntary choice, and tend to reveal the privacies of life.[149] The first prong recognizes that in *Carpenter*, the Court retained the third-party doctrine's application to pre-digital records, but suggested that records created by digital technology are categorically different.[150] The second prong emphasizes the importance of voluntary disclosure in the third-party doctrine.[151] In *Carpenter*, the Court found that because virtually any use of a smartphone generates CSLI, "in no meaningful sense does [a smartphone] user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements."[152] The last prong requires that the data searched "must be of a kind that tends to reveal an intimate portrait of a person's life typically beyond legitimate

---

144. Roberts v. U.S. Jaycees, 468 U.S. 609, 620 (1984).

145. *Id.* at 622.

146. *Id.* at 620.

147. *Id.* The Court then lists possible relevant factors to consider in determining whether an organization qualifies as an intimate association, including its size, purpose, policies, selectivity, congeniality, or other pertinent characteristics. Using these factors, the Court found that the organization fell "outside of the category of relationships worthy of this kind of constitutional protection." *Id.*

148. KERR, *supra* note 87 (manuscript at 3).

149. *Id.*

150. *Id.* (manuscript at 16).

151. *Id.* (manuscript at 20).

152. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (quotations and alterations omitted).

state interest."[153] These privacies of life include a person's "familial, political, professional, religious, and sexual associations."[154] If all prongs have been met, the information is *Carpenter*-protected, and government access to that information is deemed a search requiring a warrant.[155] This rule has the advantage of clarity, but as Kerr acknowledges, it is over-inclusive as a result.[156]

Kerr's general approach is sound, especially as to the first and third prongs. But the voluntary choice prong has vulnerabilities because it seems to depend entirely on how the record is generated and not what the record actually is. Kerr is correct that the CSLI in *Carpenter* was not generated in a meaningfully voluntary way because smartphones are constantly relaying data to cell towers without any affirmative action by the user. But how would this logic apply to home smart devices? Is asking an Amazon Echo a question (and thus triggering the creation of an audio record) a sufficiently voluntary choice? Does flushing a toilet count as a voluntary choice if the user has a smart water meter installed?

Imagine two competing smart vacuum brands. One is fully automated: it cleans, scans, maps, and recharges all on its own. The other will only clean if the user utters a wake word or pushes a button. Under Kerr's approach, the first vacuum would be legally protected because the record collection occurs without meaningful voluntary choice. But the second one would presumably not be protected because the user initiates the data collection and record creation. A device-based approach makes the constitutional rights of a person dependent upon their choice of vacuum brand. This approach does not align with the privacy principles inherent in the Fourth Amendment, especially because automated devices may be more expensive than non-automated alternatives.

C. The Data-Type-Based Approach

When creating a doctrine for assessing searches of smart devices, courts should analyze the types of data collected by smart devices, not the type of device or the method of data collection.[157] The Sonicare Flexcare Platinum Connected Toothbrush tracks the movement and pressure of the toothbrush on teeth and

---

153. KERR, *supra* note 87 (manuscript at 22).

154. *Carpenter*, 138 S. Ct. at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

155. KERR, *supra* note 87 (manuscript at 40).

156. *Id.* (manuscript at 28).

157. Professor Andrew Guthrie Ferguson suggests a reinterpretation of the Fourth Amendment's protection of "effects" to include both physical objects and data stored on and transmitted by the device. Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 853 (2016). Under Ferguson's conception of "digital curtilage," a "smart" effect includes data and signals that are: closely associated with the smart device; claimed as secure from others; and used to promote personal autonomy, family, self-expression, and association. *Id.* at 866–67. Ferguson argues that the constitutionally relevant "thing" of a smart device is not the device itself, but the data that emanates from it. *Id.* at 858–59. The essence of a smart device is not merely its sensors and plastic parts, it is the data that enables it to be "smart" in the first place. *Id.*

provides brushing insights via a smartphone app.[158] The data collection process requires exact real-time location tracking to pinpoint how the user is brushing every single tooth.[159] Because technology is rapidly evolving, and new iterations of smart devices come with the capability to collect new data types, a device-centered approach would be inconsistent and leave homeowners "at the mercy of advancing technology."[160]

This is especially true for companies that are not fully transparent about a device's capabilities. In early 2019, Google announced that its home security system, the Nest Guard, would be able to act as a digital assistant that could respond to voice commands following a software update.[161] But, for the 18 months the device had been on the market prior to this announcement, the technical specifications never mentioned the presence of a microphone.[162] Google claims the omission was an error and insists the microphone can only be enabled specifically by users.[163] If the device actually was collecting audio data that could be turned over to police, how would courts assess whether the user had a reasonable expectation of privacy? The user did not knowingly avail themselves of audio data collection, but they did avail themselves of Nest Guard's other forms of data collection like motion sensing.[164] Supposing the microphone was properly disclosed, a device-based approach could result in a user's privacy expectations as to the collection of all data types being relinquished by the collection of one data type.

In contrast to a device-based approach, an approach centered on the different categories of information is relatively more stable. Devices can evolve in unexpected ways or contain unanticipated capabilities, but genres of information will remain largely the same. Although location data is now being collected by smartphones, thermostats, and toothbrushes; the data collected still seeks to reveal the physical location of the device. Of course, location data can be collected by different methods (GPS, CSLI, etc.), but it still fits under the broader category of "location data" because it seeks to answer the same question: where was this device at a given time? Similarly, audio data can be captured by many different kinds of devices and methods, but the *object* of the data collection is the same: sound. If we know what the object of data collection is, we also know what is not collected. Audio data reveals information about sound, without revealing other data categories like location, temperature, humidity, or blood sugar concentration. Although we may

---

158. *Philips Introduces a Real-Time Data Collection & 3D Mapping Smart* Toothbrush, ECLIPSE AUTOMATION, http://www.eclipseautomation.com/philips-introduces-a-real-time-data-collection-3d-mapping-smart-toothbrush/ (last visited Apr. 21, 2019).

159. *Id.*

160. Kyllo v. United States, 533 U.S. 27, 35–36 (2001).

161. Dave Lee, *Google Admits Error over Hidden Microphone*, BBC NEWS (Feb. 20, 2019), https://www.bbc.com/news/technology-47303077; Taylor Telford, *Google Failed to Notify Customers it Put Microphones in Nest Security Systems*, WASH. POST (Feb. 20, 2019), https://www.washingtonpost.com/business/2019/02/20/google-forgot-notify-customers-it-put-microphones-nest-security-systems/.

162. Telford, *supra* note 161.

163. *Id.*

164. *See Privacy Statement*, *supra* note 139.

start seeing audio collection capabilities in unexpected places,[165] we still have a reasonable knowledge of what information can be discovered through audio recordings.

A data-type-based approach is not as difficult to implement as it may first seem. Courts have grappled with the subjectivity of *Katz* since the decision came down in 1967, and this Note simply argues that courts can apply *Katz*'s reasonable expectation doctrine to the different types of digital information that exist today. The major question remains whether a certain type of information has the capability to reveal a home's intimate details which are susceptible to government abuse.[166] Justice Sotomayor, concurring in *Jones*, was concerned that searches of GPS data could reveal "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar, and on and on."[167] The information collected by smart devices could reveal insights about the same kinds of intimate private details. An Amazon Echo's audio recordings could reveal inquiries like "Alexa, how can I get an abortion?" and a Furbo[168] pet camera's video recordings could reveal a Qur'an sitting on the living room table.[169] *Carpenter* suggests that the new third-party doctrine's scope is limited to protecting records that reveal an intimate portrait of a person's life because those records are most vulnerable to government abuse and in greatest need of increased legal protection.[170]

Can we predict which data types are likely to expose a person's intimate or private details before searching that data? This Note argues the answer is clearly yes. The Court has already determined that location data, in the forms of GPS and CSLI, has a great likelihood of exposing these intimate details.[171] Audio and visual data certainly has the ability to expose an embarrassing or private piece of

---

165. Take for example My Friend Cayla, a smart doll which uses voice recognition technology that allows children to access the Internet. Philip Oltermann, *German Parents Told to Destroy Doll That Can Spy on Children*, THE GUARDIAN (Feb. 17, 2017, 11:53 PM), https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children. The German government classified this doll as an "illegal espionage apparatus," and mandated that retailers and owners destroy or permanently disable the doll's smart capabilities. *Id.*

166. *See* United States v. Di Re, 332 U.S. 581, 595 (1948) ("[T]he forefathers, after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of some criminals from punishment.").

167. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (quoting People v. Weaver, 12 N.Y.3d 433, 441–42 (2009)).

168. FURBO, https://shopus.furbo.com/ (last visited Apr. 21, 2019).

169. If the Court is worried about the government obtaining knowledge of a person's "familial, political, professional, religious, and sexual associations" through tracking their public movements, data revealing those same associations that is generated within the confines of the home would presumably be more protected. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

170. KERR, *supra* note 87 (manuscript at 26).

171. *Carpenter*, 138 S. Ct. at 2217 (quoting Riley v. California, 573 U.S. 373, 403 (2014)).

information. Biometric data about the inner workings of the body involves private information that is about as intimate as one can get.[172] The government's knowledge of these types of information puts a person in danger of abuse or exploitation.[173] But what if the government learns how fast you eat your food using a smart fork?[174] How long you cook your stew?[175] Whether you left the refrigerator door open?[176] The narrow glimpse these pieces of data offer into a person's life do not expose them to the same level of police abuse, and thus these data types should not demand the same level of legal protection.

Does precedent support allowing a court to pick and choose between which categories of information it deems most sensitive? Justice Scalia's opinion in *Kyllo* rejected this piecemeal approach.[177] The Court rejected limiting the prohibition on the warrantless use of thermal-imaging devices by police to "intimate details" of a home's interior.[178] A thermal imager might be able to detect an intimate detail, like what time a person in the house takes a bath, and also a trivial detail like a closet light being left on.[179] Justice Scalia said it would be unworkable to develop a jurisprudence "specifying which home activities are 'intimate' and which are not."[180] *Kyllo* appears to prefer a binary between private information and non-private information when assessing the constitutionality of a warrantless search with no consideration of intimacy.[181] This means that even trivial information like a

---

172. The Fourth Amendment's first enumerated object of protection from warrantless search is "persons." U.S. CONST. amend. IV; *see also* Maryland v. King, 569 U.S. 435, 469 (2013) (Scalia, J., dissenting) ("But why are the 'privacy-related concerns' not also 'weighty' when an intrusion into the *body* is at stake?").

173. *See* United States v. Rabinowitz, 339 U.S. 56, 69 (1950) (Frankfurter, J., dissenting) ("[T]he central fact about the Fourth Amendment . . . [is] that it was a safeguard against recurrence of abuses so deeply felt by the Colonies as to be one of the potent causes of the Revolution."); Daniel S. Jonas, Comment, *Pretext Searches and the Fourth Amendment: Unconstitutional Abuses of Power*, 137 U. PA. L. REV. 1791, 1797 (1989) ("[T]he abuses that the fourth amendment was designed to prevent exist now as they did two centuries ago; the historical purposes of the fourth amendment have relevance beyond mere academic interest.").

174. HAPI.COM, https://www.hapilabs.com/product/hapifork (last visited Apr. 21, 2019).

175. *Crock-Pot 6-Quart WeMo-Enabled Smart Slow Cooker, Stainless Steel*, AMAZON, https://www.amazon.com/Crock-Pot-Wifi-Enabled-Cooker-6-Quart-Stainless/dp/B00IPEO02C (last visited Apr. 21, 2019).

176. Shannon Liao, *Samsung's New Fridge Will Ping Your Phone if You Leave the Door Open*, THE VERGE (Jan. 7, 2019, 5:00 PM), https://www.theverge.com/2019/1/7/18169342/samsung-family-hub-4-fridge-washer-bixby-ces-2019.

177. Kyllo v. United States, 533 U.S. 27, 38–39 (2001) (quoting Oliver v. United States, 466 U.S. 170, 181 (1984)).

178. *Id.* at 38.

179. *Id.*

180. *Id.* at 38–39.

181. *Id.* at 38–40.

person's hair brushing technique[182] demands the same level of protection as the floorplan of a person's apartment.[183]

But *Carpenter* seems to eliminate this binary and replace it with a hierarchy.[184] Orin Kerr suggests that the Court adopted Timothy Carpenter's assertion that the third-party doctrine "diminishes" an expectation of privacy, but does not destroy it.[185] The Court clarified that the information sought in *Smith* and *Miller* could still be searched without a warrant, but intimate and comprehensive CSLI data demanded a warrant prior to searching.[186] Aside from this shift in the Court's perception of privacy, *Kyllo*'s rejection of an intimacy standard might not be persuasive in light of the capabilities of smart devices. The Court was concerned that an intimacy standard would fail to give police notice over whether a particular device revealed unduly intimate details.[187] But the technology governing smart device data collection is much more sophisticated than the relatively crude thermal imagers in *Kyllo*.[188] When subpoenaing a device company for information, the police would know in advance what data types they seek.[189] By subpoenaing L'Oréal for a smart hairbrush's gyroscopic data, the police run no risk of accidentally collecting much more intimate information like the interior layout of a home.

D. Data Types and Analysis

Because smart devices could collect hundreds of different types of data it would be impractical to analyze each one. Instead, this Section will offer insights into some categories to see how courts could differentiate the privacy interests inherent in those data types. This Section examines audio data, "home-layout

---

182. Lucy Handley, *L'Oreal's Smart Brush 'Listens' to Hair, Recommends Luxury Treatments*, CNBC (Jan. 4, 2017, 6:29 AM), https://www.cnbc.com/2017/01/04/lorealssmart-brush-listens-to-hair-recommends-luxury-treatments.html.

183. Maggie Astor, *Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared*, N.Y. TIMES (July 25, 2017), https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html.

184. Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE (June 22, 2018, 1:18 PM), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision.

185. *Id.*

186. Carpenter v. United States, 138 S. Ct. 2206, 2220–21 (2018) ("We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras.").

187. Kyllo v. United States, 533 U.S. 27, 38–39 (2001).

188. *Id.* at 36. It is also important to note that *Kyllo* did not involve the third-party doctrine. The Court's initial rejection of an intimacy standard did not explicitly apply to the third-party doctrine, but it is indicative of how the Court understands its role in developing a workable jurisprudence.

189. This would also conform with the Fourth Amendment's requirement that a warrant "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

data,"[190] smartphone alerts, and data types that provide only trivial amounts of information about a person.

1. Audio Data

Many of the most popular smart devices operate by voice command, including the Amazon Echo and Google Home smart speakers,[191] the Samsung Smart TV,[192] and the Honeywell Wi-Fi Smart Thermostat.[193] The Amazon Echo, arguably the most popular smart speaker, offers an interesting case study.[194] The Echo is always listening, but it is not always cataloguing audio data and transmitting it back to Amazon.[195] Upon the utterance of a "wake word" like "Alexa" or "Echo," the device begins recording a user's audio command.[196] The device responds to the user's commands, and audio recordings are sent to Amazon employees who listen to them and use the data to refine Echo's speech recognition capabilities.[197] Amazon claims that the Echo only records audio data after a wake word is uttered and does not collect and store all audio heard by the device.[198]

---

190. This Note uses the term "home-layout data" to refer to graphical, but not necessarily photographic depictions of a home's interior.

191. Tim Moynihan, *Alexa and Google Home Record What You Say. But What Happens to That Data?*, WIRED (Dec. 5, 2016, 9:00 AM), https://www.wired.com/2016/12/alexa-and-google-record-your-voice/.

192. Nicole Nguyen, *If You Have a Smart TV, Take a Closer Look at Your Privacy Settings*, CNBC (Mar. 9, 2017, 7:08 PM), https://www.cnbc.com/2017/03/09/if-you-have-a-smart-tv-take-a-closer-look-at-your-privacy-settings.html.

193. *Wi-Fi Smart Thermostat with Voice Control (RTH9590WF)*, HONEYWELL HOME, https://www.honeywellhome.com/en/products/heating-and-cooling/wi-fi-smart-thermostat-with-v-rth9590wf (last visited Apr. 21, 2019).

194. Leena Rao, *Amazon is Dominating the Voice-Assisted Speaker Market*, FORTUNE (May 8, 2017), https://fortune.com/2017/05/08/amazon-echo-alexa-speakers/.

195. John Kruzel, *Is Your Amazon Alexa Spying on You?*, POLITIFACT (May 31, 2018, 10:00 AM), https://www.politifact.com/truth-o-meter/statements/2018/may/31/ro-khanna/your-amazon-alexa-spying-you/.

196. *Id.*

197. Jordan Valinsky, *Amazon Reportedly Employs Thousands of People to Listen to Your Alexa Conversations*, CNN (Apr. 11, 2019, 2:38 PM), https://www.cnn.com/2019/04/11/tech/amazon-alexa-listening/index.html.

198. But, one Echo user reported an incident where her device mistakenly heard a wake word, started recording her conversation, and sent the audio to a contact on her phone list. Amazon claims this was an "extremely rare occurrence." Sam Wolfson, *Amazon's Alexa Recorded Private Conversation and Sent It to Random Contact*, THE GUARDIAN (May 24, 2018), https://www.theguardian.com/technology/2018/may/24/amazon-alexa-recorded-conversation. Leaked audio recordings collected by the Google Home smart speaker also revealed that sensitive conversations were collected by the device without being prompted by a wake word, including "bedroom conversations, conversations between parents and their children, but also blazing rows and professional phone calls containing lots of private information." Jon Brodkin, *Google Workers Listen to Your "OK Google" Queries–One of Them Leaked Recordings*, ARS TECHNICA (July 11, 2019, 12:31 PM), https://arstechnica.com/information-technology/2019/07/google-defends-listening-to-ok-google-queries-after-voice-recordings-leak/.

While this is the current status of the Echo's audio data collection process, Amazon filed a patent in 2017 for a "voice sniffer algorithm" that would use Echo to listen for trigger words like "prefer," "bought," or "disliked" along with an adjacent keyword.[199] This information would then be sent to advertisers to target ads to the user based on the content of their conversations.[200] For example, the device may hear audio like "When we went to southern California, I fell in **love** with Santa Barbara. There were so many **great** wineries to visit."[201] The algorithm could then associate positive traits to Santa Barbara and wine, and then share that information with Santa Barbara travel agents or wine companies. Amazon claims that its patent filings do not necessarily indicate its future business plans,[202] but if this voice sniffer algorithm became standard, it could pose a threat to the legal privacy rights of users. If police are able to access a catalogue of all conversations passively collected in a home without a warrant, they would have access to an encyclopedic knowledge of a person's private conversations.

Audio recordings by Echo devices are already being sought by police to solve crimes. In 2015, Victor Collins died in a hot tub inside the home of James Bates in Bentonville, Arkansas.[203] As part of an investigation into Collins's death, police charged Bates with murder and sought audio recordings from an Echo that Bates had in his kitchen, hoping it might have recorded audio from that night.[204] Amazon initially resisted sharing the data, arguing that the data is speech protected by the First Amendment,[205] but eventually shared it after Bates agreed to release the data.[206] After reviewing the audio data, as well as data obtained from a smart utility

---

199. Andrea Miller, *Amazon Patent Reveals 'Voice Sniffer Algorithm' That Could Analyze Conversations*, ABC NEWS (Apr. 3, 2018, 3:54 PM), https://abcnews.go.com/Business/amazon-patent-reveals-voice-sniffer-algorithm-analyze-conversations/story?id=54175793.

200. *Id.*

201. Sapna Maheshwari, *Hey, Alexa, What Can You Hear? And What Will You Do with It?*, N.Y. TIMES (Mar. 31, 2018), https://www.nytimes.com/2018/03/31/business/media/amazon-google-privacy-digital-assistants.html.

202. Miller, *supra* note 199.

203. Colin Dwyer, *Arkansas Prosecutors Drop Murder Case That Hinged on Evidence from Amazon Echo*, NPR (Nov. 29, 2017, 5:42 PM), https://www.npr.org/sections/thetwo-way/2017/11/29/567305812/arkansas-prosecutors-drop-murder-case-that-hinged-on-evidence-from-amazon-echo.

204. *Id.*

205. Thomas Brewster, *Amazon Argues Alexa Speech Protected by First Amendment in Murder Trial Fight*, FORBES (Feb. 23, 2017, 7:10 AM), https://www.forbes.com/sites/thomasbrewster/2017/02/23/amazon-echo-alexa-murder-trial-first-amendment-rights/#72d84c665d81. For a discussion of whether the First Amendment protects the speech of artificial intelligence, *see generally* Toni M. Massaro & Helen Norton, *Siri-ously? Free Speech Rights and Artificial Intelligence*, 110 NW. U. L. REV. 1169 (2016).

206. Dwyer, *supra* note 203.

meter installed in the house,[207] prosecutors dropped the case against Bates, stating that the evidence could support multiple reasonable explanations.[208]

In November 2018, a New Hampshire judge ordered Amazon to hand over the Echo recordings from a suspected murder scene after a woman was stabbed to death in her kitchen.[209] Currently, Amazon's policy is that it "will not release customer information without a valid and binding legal demand properly served on [Amazon]. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course."[210] Without further illumination from the courts, the privacy of smart device data relies on the internal policies of the businesses which collect that data,[211] and a subpoena will be enough compulsion for most businesses to cooperate.[212]

2. Home-Layout Data

Home-layout data refers to data that is created by smart devices that gives a visualization of the interior layout of a home. One popular smart device that creates home-layout data is the iRobot Roomba smart vacuum.[213] The Roomba uses smart

---

207. *See* Zuzanna Sitek & Dillon Thomas, *Bentonville PD Says Man Strangled, Drowned Former Georgia Officer*, KSFM 5NEWS ONLINE (Feb. 23, 2016, 10:43 PM), https://5newsonline.com/2016/02/23/bentonville-pd-says-man-strangled-drowned-former-georgia-officer/. The smart utility meter was installed by the Bentonville Utilities Department. This data showed that 140 total gallons of water were used in a span of two hours. Police concluded that this unusual amount of water was used to clean up the scene. Bates also owned "a Nest thermostat, a Honeywell alarm system, wireless weather monitoring in the backyard, and WeMo devices for lighting at the smart home crime scene." But it is unclear whether police searched any of these devices as part of their investigation. Max Brantley, *Bentonville Police Try to Tap High-Tech Devices for Murder Case Clues*, ARK. TIMES (Dec. 28, 2016, 9:39 AM), https://www.arktimes.com/ArkansasBlog/archives/2016/12/28/bentonville-police-try-to-tap-high-tech-devices-for-murder-case-clues.

208. Dwyer, *supra* note 203.

209. Cyrus Farivar, *Amazon Must Give up Echo Recordings in Double Murder Case, Judge Rules*, ARS TECHNICA (Nov. 10, 2018, 4:35 AM), https://arstechnica.com/tech-policy/2018/11/amazon-must-give-up-echo-recordings-in-double-murder-case-judge-rules/. Aside from the audio files, the judge also required Amazon to disclose associated data, such as which phones were paired to the Echo, that may be connected to the homicides.

210. Brewster, *supra* note 205.

211. As Jennifer Granick, the surveillance and cybersecurity counsel for the ACLU says, "[w]e're depending on companies to be the intermediary between people and the government." Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html?action=click&module=Top%20Stories&pgtype=Homepage.

212. *See* Orin Kerr, *Does Carpenter Revolutionize the Law of Subpoenas?*, LAWFARE (June 26, 2018, 6:44 PM), https://www.lawfareblog.com/does-carpenter-revolutionize-law-subpoenas ("The only constitutional limit now is that the possessors of the evidence can try to assert their modest Fourth Amendment objections based on the burdensomeness of complying with the subpoena. But in most cases that's a very limited objection.").

213. Ackerman & Guizzo, *supra* note 109.

navigation technology named VSLAM (Vision Simultaneous Localization and Mapping) to optimize the vacuum's transit through a home.[214] The vacuum's sensors map out a person's home, identifying furniture, surfaces, and obstacles to determine where it has been and where it has not.[215] As iRobot CEO Colin Angle explains, "we can create digital representations of what a home looks like so our robots can be smarter."[216] This digital representation of a home's interior goes beyond just an architectural blueprint of the home, it can help iRobot determine what appliances a resident has, and which room belongs to a child.[217] These visual representations are generated by an algorithm without permanently recording a single photographic image.[218] From a business standpoint, home-layout data could be extremely valuable to iRobot and other smart vacuum brands who want to sell such data to advertisers.[219]

Home-layout data may endanger the inviolability of the home in Fourth Amendment jurisprudence because it has the potential to turn confidential details about a home's interior "inside out."[220] The Court places the security of the home at the forefront of Fourth Amendment jurisprudence, drawing a firm and bright line at the entrance to the home.[221] An officer's access to the detailed digital representation of a home's interior generated by a Roomba is tantamount to the officer physically crossing the threshold of a home's entrance. This kind of search is merely a subtler form of the prototypical British officer breaking into a colonist's home to search for

---

214. *Id.*

215. *Id.* See accompanying videos for a demonstration of how the vacuum maps out the interior of a house.

216. *Id.*

217. Rhett Jones, *Roomba's Next Big Step is Selling Maps of Your Home to the Highest Bidder*, GIZMODO (July 24, 2017, 2:05 PM), https://gizmodo.com/roombas-next-big-step-is-selling-maps-of-your-home-to-t-1797187829 ("Just remember that the Roomba knows what room your child is in, it's the one where it bumps into all the toys on the floor.").

218. Wetmore, *supra* note 111. According to iRobot, newer models of their robotic vacuums will work off of low-resolution camera images that mostly capture vague areas of light and shade. James Vincent, *Google Wants to Improve Your Smart Home with iRobot's Room Maps*, THE VERGE (Oct. 31, 2018, 9:00 AM), https://www.theverge.com/2018/10/31/18041876/google-irobot-smart-home-spatial-data-mapping-collaboration.

219. Google says that the data collected by iRobot would not be used in Google's advertising business, and that the data "is not getting fed into some larger morass of Google information." *Id.* The companies note that Google will not access any of the 3D or spatial information collected by the device, but Google will collect home-layout information in an indirect way. *Id.* Although Google will not receive a graphical depiction of a home's kitchen, it will learn which area in the home a user has labeled as the kitchen. *Id.* This information still assists Google in laying the foundation for future integrated smart home systems and products. *Id.*

220. Astor, *supra* note 183.

221. Kyllo v. United States, 533 U.S. 27, 40 (2001) (citing Payton v. New York, 445 U.S. 573, 590 (1980)).

evidence of sedition.[222] The Court should recognize the power of home-layout data to reveal a home's intimate details, and accordingly protect that data by requiring police to obtain a warrant before accessing it.

3. "Mere Alerts"

Smart devices can often communicate with each other by sending alerts or notifications to a smartphone or other device. The Griffin Connected Toaster can send a notification to the user's smartphone when their bread is done toasting.[223] The Samsung Family Hub 4.0 refrigerator will send a notification when a user leaves the refrigerator door open.[224] Does this transmission of a notification from one device to another necessarily invoke Fourth Amendment protection? In November 2018, the Seventh Circuit ruled that it does not. In *United States v. Brixen*, the defendant arranged to meet with a supposed underage girl over the image-sharing social media app Snapchat and was arrested at the rendezvous point.[225] In custody, the undercover officer with whom the defendant had been unknowingly communicating sent a message from the underage girl persona's account and a visual notification appeared on the defendant's phone screen.[226] The Seventh Circuit held that this was not a search, and the triggering of a notification was reasonable because unlike *Riley*, the mere pop-up of a notification did not involve "affirmatively accessing the content within cell phones," and because the defendant was in custody, he retained no privacy interest in what appeared in plain view on the phone's screen.[227]

Riley suggests such "mere alerts" do not invoke Fourth Amendment privacy concerns when law enforcement officers refrain from accessing or manipulating the content of smart devices.[228] If an officer seeks to confirm that an individual owns a certain smart device, they may trigger an alert to that person's smartphone without running afoul of the Fourth Amendment. But some devices could exist where the process of sending an alert necessarily involves gaining access to and manipulating the device's digital content. In these cases, the rule from *Riley* would apply, and a warrant is necessary.

4. De Minimis *Data Types*

Not all data types collected by smart devices carry the danger of exposing a person's privacies of life. These data types may be so minimally intrusive as to be considered *de minimis*.[229] These data types inherently carry a low likelihood of

---

222. *See Payton*, 445 U.S. at 583 (1980) ("It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment.").

223. Baldwin, *supra* note 113.

224. Liao, *supra* note 176.

225. United States v. Brixen, 908 F.3d 276, 278–79 (7th Cir. 2018).

226. *Id.* at 279.

227. *Id.* at 281.

228. *Id.* at 282.

229. Ingraham v. Wright, 430 U.S. 651, 674 (1977) ("There is, of course a de minimis level of imposition with which the Constitution is not concerned."). *See generally*

exposing a person's "familial, political, professional, religious, and sexual associations."[230] The Meater Smart Meat Thermometer can connect with a user's smartphone and send internal temperature readings during the cook time.[231] The "meat temperature" data type can only reveal so much about a person. The revelation that a piece of steak was cooking at 135 degrees Fahrenheit could explain how a person likes their steak, but it does not risk exposing that person's religious or sexual associations. The HAPIfork is a smart fork designed to help people lose weight and solve digestive problems by measuring a person's eating speed.[232] Knowing how fast someone moves a fork from plate to mouth is such a trivial glimpse into a person's life that it should not be considered to invoke the same privacy interests as location data. The same logic applies to a smart egg carton that tracks the number of eggs a person has in their refrigerator,[233] or a toaster that can measure a user's "toast-cooking profile."[234] The inherent triviality of these data types should lead a court to conclude that a person has such a low privacy interest that a warrantless search would be reasonable.[235]

CONCLUSION

This Note proposes that a court asked to decide the constitutionality of the government's warrantless access to data collected by a smart device should start by determining what type of data the information is. The court should then determine whether this particular data type has the tendency to reveal an intimate fact about the user which is susceptible to government abuse. If it does, the Court should declare that particular data type is protected by the Fourth Amendment's warrant requirement. If not, a warrantless search is reasonable. As more categories receive judicial inquiry over time, a hierarchy of data protection will develop that reflects society's reasonable expectations of privacy.

A simple solution to all of this murky doctrine would be to abolish the third-party doctrine altogether. Without the third-party doctrine, courts would not have to differentiate the relative privacy protections of data types, or question how many days' worth of CSLI collection is sufficient to trigger a Fourth Amendment

---

Jeffrey Brown, *How Much is Too Much? The Application of the* de minimis *Doctrine to the Fourth Amendment*, 82 MISS. L.J. 1097 (2013).

230. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

231. *See* MEATER, https://meater.com/ (last visited Apr. 21, 2019).

232. HAPI.COM, *supra* note 174.

233. Natt Garun, *Egg Minder Smart Tray Lets You Remotely Check the Freshness of Your Eggs*, DIGITAL TRENDS (July 5, 2013, 8:06 AM), https://www.digitaltrends.com/home/egg-minder-smart-tray-lets-you-remotely-check-the-freshness-of-your-eggs/.

234. Baldwin, *supra* note 113.

235. In United States v. Jacobsen, the Court held that police may take a small sample of white powder found in a package damaged in transit to test it for the presence of contraband without a warrant. United States v. Jacobsen, 466 U.S. 109, 111, 125 (1984). The Court explained that in circumstances like this, "the safeguards of a warrant would only minimally advance Fourth Amendment interests. This warrantless 'seizure' was reasonable." *Id.* at 125.

search. Perhaps a doctrine developed from cases involving phone booths and pen registers has outlived its usefulness in a digital world increasingly driven by data collection.[236] At least one justice believes that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[237] Another justice suggests that the "best solution to privacy concerns may be legislative."[238] But as long as the Court maintains the doctrine, it should craft rules that account for a person's reasonable expectations of privacy by delineating which distinct categories of information the doctrine covers, and which it does not extend to.[239] Chief Justice Roberts's simple advice in *Riley* about what police must do before searching a cell phone ought to be the same rejoinder when police seek to search smart devices in a person's home: "get a warrant."[240]

---

236. Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1945 (2017).

237. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

238. *Id.* at 429 (Alito, J., concurring); *see, e.g.*, Dalvin Brown, *California 'Anti-Eavesdropping' Bill Seeks to Regulate Smart Speakers*, USA TODAY (May 29, 2019, 11:25 AM), https://www.usatoday.com/story/tech/2019/05/29/alexa-smart-speakers-face-regulation-through-calif-bill/1268363001/; Nick Sibilla, *Utah Bans Police from Searching Digital Data Without a Warrant, Closes Fourth Amendment Loophole*, FORBES (Apr. 16, 2019, 11:25 AM), https://www.forbes.com/sites/nicksibilla/2019/04/16/utah-bans-police-from-searching-digital-data-without-a-warrant-closes-fourth-amendment-loophole/#6afa20b57630; Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015, 9:58 PM), https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/.

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

240. Riley v. California, 573 U.S. 373, 403 (2014).

***