VOLUME 5 December 2023 ISSUE 1

JOURNAL ON EMERGING TECHNOLOGIES

NOTES

PRIVACY IN THE AGE OF IoT TECHNOLOGIES: EXAMINING THE SHORTCOMING OF THE FOURTH AMENDMENT AND THE THIRD-PARTY DOCTRINE FOR SMART HOME USERS

Perla Khattar & Dillon B. Yang

ABSTRACT

The Fourth Amendment gives people the right to be secure in their house from unreasonable searches and seizures. But, as with most things, there are exceptions. For example, the third-party doctrine holds that the Fourth Amendment does not protect information that has been revealed to third parties. With the stark rise in IoT smart home technologies, law enforcement may be able to bypass the warrant requirement with the third-party doctrine and access sensitive in-home data through companies like Amazon and Google. Interestingly, the Supreme Court has repeatedly held that the home is sacred, and it is at the core of Fourth Amendment protections. Consequently, IoT smart home technologies have put Fourth Amendment jurisprudence on a collision course with the third-party doctrine.

This piece contends (as many others have) that the Fourth Amendment must stretch to protect the data generated within a smart home, thus creating an exception to the third-party doctrine. But, this piece goes further than that. Because of the vast types and complexities of IoT smart home technologies, a "bright-line" test cannot fix the collision between the third-party doctrine and Fourth Amendment jurisprudence. This collision needs a nuanced solution that accounts for the many types of IoT smart home technologies.

PRIVACY IN THE AGE OF IOT TECHNOLOGIES: EXAMINING THE SHORTCOMING OF THE FOURTH AMENDMENT AND THE THIRD-PARTY DOCTRINE FOR SMART HOME USERS

Perla Khattar[*†] *& Dillon B. Yang*[**†]

INTRODUCTION

In late 2018, a New Hampshire judge ordered Amazon.com LLC to hand over private data from an Echo smart speaker device located in a house where the alleged double murder of Christine Sullivan and Jenna Pellegrini took place.[1] Prosecutors believed that the Echo device might have contained useful information that could help make a case against the prime suspect Timothy Verrill.[2] However, this case alongside others raises concerns regarding the ease with which law enforcement agencies are able to access private data from one's home. With the rise in popularity of smart home technologies, police are gaining access to data stored on companies' remote clouds without proving probable cause. In many cases, police are able to access the needed data by serving the companies a subpoena, a court order, or by completing a form on the company's website.[3] In fact, Amazon has a webpage where law enforcement can fill out a form to get access to data without user-consent.[4] In 2022, Amazon handed over eleven Ring doorbell captured videos to law enforcement through this "consentless shortcut."[5]

When the Fourth Amendment to the U.S. Constitution was passed

---

[*] Attorney at Beirut Bar & J.S.D. Candidate 2026, Notre Dame Law School.
[**] Judicial Law Clerk at U.S. District Courts & J.D. 2023, Notre Dame Law School.
[†] These authors contributed equally to this work and share first authorship.
Perla Khattar and Dillon Yang thank Assistant U.S. Attorney & Adjunct Professor of Law John Maciejczyk for advising this Note and providing excellent guidance. Professor M. sparked our interest in the intersection of technology and the Fourth Amendment in his Cybercrime Law class.
[1] Chavie Lieber, *Amazon's Alexa Might Be a Key Witness in a Murder Trial*, VOX (Nov. 12, 2018), https://www.vox.com/the-goods/2018/11/12/18089090/amazon-echo-alexa-smart-speaker-privacy-data.
[2] *Id.* at 2.
[3] Sean Hollister, *Today I Learned Amazon Has a Form So Police Can Get My Data Without Permission or a Warrant*, THE VERGE (Jan. 14, 2022), https://www.theverge.com/2022/7/14/23219419/amazon-ring-law-enforcement-no-warrant-no-consent.
[4] *Id.*
[5] *Id.*

in 1791, it was primarily regarded as a response to the English rule whereby British officials could conduct warrantless searches of citizens' homes. To prevent similar abuses by the new American government, and to respect the highly regarded value of privacy, the Fourth Amendment required searches and seizures to be supported by a judge-issued warrant, based on probable cause. However, the modern home today does not resemble the home that the Founders knew when passing the Fourth Amendment. Instead of looking through peepholes to see who's standing at the door, Americans can now open an application on their phone that's connected to a smart doorbell camera. Instead of calling the weather station, Alexa and Google Assistant are always on standby ready to answer the most intricate questions. Instead of stoking a fireplace, smart thermostats allow homeowners to control the temperature of their house from miles away. While these technologies provide users with convenience, they also export massive amounts of data to third-party servers. The Fourth Amendment, once regarded as the protector of American homes' sanctity, is now unable to keep up with the latest technological advancements.

This piece contends that the variety and complexity of smart home technologies afford a nuanced response to the collision between the Fourth Amendment and the third-party doctrine. Part I discusses the landscape and varieties of current smart home technology. Part II explains how smart home technology has already been labeled as invasive in the consumer data protection world through enforcement orders and lawsuits. Part III surveys the relevant intersecting lines of the Fourth Amendment regarding the jurisprudence generally, technological advancements, and the third-party doctrine. Part IV demonstrates that the variety of smart home technology warrants Fourth Amendment protection in some cases and not others.

I. THE LANDSCAPE OF SMART HOME TECHNOLOGY TODAY

Smart home Internet of Things ("IoT") technologies incorporate artificial intelligence into homes and residences that seek to optimize safety, convenience, and energy conservation.[6] Automated appliance control and general assistive technology offer a better quality of life when incorporated into the architecture of dwellings. Smart monitoring and access control optimize security, automation offers heightened

[6] *See* Muhammad Raisul Alam, et al., *A Review of Smart Homes—Past, Present, and Future*, 42 IEEE TRANSACTIONS ON SYS., MAN., & CYBERNETICS 1190, 1190–1203 (2012).

convenience, and ambiance intelligence systems enhance energy conservation.

The most relevant technologies for smart homes are Wake Word Technology ("WWT"), Integrated Wireless Technology ("IWT"), Smart Home Micro-computers ("SMMC"), and Home Automation ("SHS/HA").[7] These technologies spawned popular devices like the Ring Doorbell, the Amazon Alexa, and the Philips Hue Bulb. However, the complexity of IoT technologies means that smart home devices are not created equal: the underlying architecture differs from one apparatus to another, and the privacy challenges are therefore unique to each device. In other words, personal information that resides on a company's remote cloud through a virtual assistant is categorically different in nature from the data collected when television is operated remotely, or a thermostat is adjusted from afar.

A. Virtual Voice Assistants and Smart Doorbell Cameras

Virtual Voice Assistant ("VVA") devices are a type of smart home technology that uses artificial intelligence to interact with its users through voice commands or text input.[8] The most common software programs on the market are Amazon's Alexa Voice Service and Google Assistant. These virtual software applications are embedded in smart speakers,[9] allowing the device to use natural language processing and machine learning algorithms to interpret user commands after hearing the wake word. A wake word, such as "Hey Alexa," is a predefined trigger phrase that initiates the device's listening mode and allows it to perform automatic speech recognition to respond to the inquiry. The trigger word, the command, and the output are transferred to the respective company's cloud where they are processed and later stored indefinitely.[10]

Smart doorbell cameras ("SDC") are security devices that combine a doorbell with a high-definition camera, equipped with night vision capabilities and motion detection sensors that capture videos of anyone

---

[7] Gabriele Lobaccaro, et al., *A Review of Systems and Technologies for Smart Homes and Smart Grids*, 9 ENERGIES 348 (2016).
[8] Michele Wojciechowski, *New Technology: Keeping It Ethical, Keeping It Legal*, AM. PHYSICAL THERAPY ASS'N (Nov. 1, 2019), https://www.apta.org/apta-magazine/2019/11/01/new-technology-keeping-it-ethical-keeping-it-legal.
[9] The Alexa Voice Service software is embedded into the Echo device, and the Google Assistant software is embedded into Google Home.
[10] *The Best Voice Assistants*, REVIEWS.COM (Sept. 9, 2021), https://www.reviews.com/home/smart-home/best-voice-assistant/.

or anything that approaches the door.[11] A branch of the IoT technologies, smart doorbell cameras have the ability to connect to the internet via Wi-Fi, allowing users to control the cameras from their smartphone or other mobile devices, and talk through the speaker.[12] Amazon owns Ring, an SDC device that supports two-way talk functionality, motion-activation, infrared night vision, and live footage streaming.[13]

The data collected by VVAs and SDCs stored on a company's cloud could become relevant to investigations in pending criminal matters. Companies operating these virtual voice assistants can be asked to produce the data for law enforcement agencies. Amazon affirms in its privacy policy that customer information is never disclosed to government entities unless required by a legally binding and valid court order or a subpoena.[14] The same terms are reiterated in Google's terms of service.[15] Further, Amazon advocated in Congress for heightened privacy laws requiring law enforcement agencies to obtain a search warrant to access the content of customer communications, rather than a subpoena or a court order.[16]

The data stored on a company's cloud could also become relevant in criminal trials. In 2015, Amazon was subpoenaed in a case where an individual was found dead, floating in a bathtub inside a house that was connected to an Echo device.[17] With a simple subpoena to a company operating a VVA or SDC, authorities are able to access voice recordings from interactions with the VVA, videos and audio files recorded by the SDC, motion detection data, records of interactions and requests made via the VVA, shortcuts added via the VVA, records of communications requests, browsing history, log of the VVA or SDC use, name, time zone, address, phone numbers linked to the account, payment information, age, personal interests, IP address, and acoustic model of voice characteristic.[18] In addition, the latest studies are proving that forms and

---

[11] C.K. Gomathy & Devulapalli Satya, *A Study on IoT Smart Doorbells*, 8 INT'L RSCH. J. ENG'G & TECH., 1470, 1473 (2008).
[12] Amanda Derrick, *What is The Ring Doorbell and How Does It Work?*, LIFEWIRE (Feb. 17, 2021), https://www.lifewire.com/how-ring-doorbell-works-4583925.
[13] *Id.*
[14] *Top Customer Questions*, AMAZON, https://www.amazon.com/b/?node=23608568011 (last visited Dec. 17, 2023) [hereinafter AMAZON].
[15] *Terms of Service*, GOOGLE, https://policies.google.com/terms/information-requests (last visited Dec. 17, 2023).
[16] *See* AMAZON, *supra* note 14.
[17] Brian Heater, *Can Your Smart Home Be Used Against You In Court?*, TECHCRUNCH (Mar. 12, 2017), https://techcrunch.com/2017/03/12/alexa-privacy/.
[18] Jason Cohen, *Amazon's Alexa Collects More Of Your Data Than Any Other Smart*

patterns are stored within a user's VVA-related data, which reveal a user's behaviors and usage patterns.[19] For example, if a user's data showed that no light has been turned on inside of their property for a week, the defense or the prosecution could bring the argument that the owner was not home for a week—an argument that could incriminate or serve as an alibi in the given scenario.

The private information and patterns that can be deduced from a simple "Hey Alexa," "Hello Google," or front door video are far too great to be handed over to authorities with a simple subpoena or court order. Users have an expectation of privacy inside of their homes and a warrant should be required to access data stored on the VVA's or SDC's cloud.

B. Other IoT Smart Home Technologies

The IoT technologies have rapidly transformed the landscape of modern homes, providing a wealth of new technological opportunities for enhancing daily life. Among these opportunities are smart thermostats, smart lighting, and smart appliances.

Smart thermostats work by using advanced built-in sensors to control and manage the heating and cooling systems in smart homes. The sensors collect data about temperature and humidity levels and send this information to the thermostat's processors to receive an output back. Over time, smart thermostats like the Nest Learning Thermostat can identify habits and preferences by analyzing daily routines. Data that is typically collected by that type of technology are temperature and humidity readings, historical data, user input, and energy usage.[20]

When it comes to smart lighting, Philips Hue is the most popular brand[21] that offers users a starter kit that includes lights, a bridge, an Ethernet cable, and a power adapter.[22] The lights are connected to the internet and users are able to control their lighting system by using the

---

Assistant, PC MAG. (Mar. 30, 2022), https://www.pcmag.com/news/amazons-alexa-collects-more-of-your-data-than-any-other-smart-assistant.

[19] Hyunji Chung & Sangjin Lee, *Intelligent Virtual Assistant knows Your Life*, ARXIV (Feb. 28, 2018), https://arxiv.org/abs/1803.00466.

[20] *Privacy Statement for Nest Products and Services*, NEST, https://nest.com/legal/privacy-statement-for-nest-products-and-services/ (last visited Dec. 17, 2023).

[21] Carrie-Ann Skinner, *How Do Smart Light Bulbs Work, And Should I Buy one?*, TECHRADAR (June 26, 2021), https://www.techradar.com/news/how-do-smart-light-bulbs-work-and-should-i-buy-one.

[22] *Hue White and Color Ambiance Starter Kit: 4 E26 Smart Bulbs (75 W)*, PHILIPS HUE, https://www.philips-hue.com/en-us/p/hue-white-and-color-ambiance-starter-kit--4-e26-smart-bulbs--75-w-/046677563295#overview (last visited Dec. 17, 2023).

application.[23] A smart light bulb may collect a variety of data depending on the specific model and manufacturer. In short, smart light bulbs can collect data on their energy consumption and usage patterns, their brightness level, color temperature, and their connectivity status.[24]

As for smart appliances, this branch of IoT technologies includes smart refrigerators, ovens, dishwashers, washing machines, coffee makers, air purifiers, televisions, and robot vacuum cleaners. These devices generally collect data that is related to the work they are trying to achieve: robot vacuums will collect cleaning schedules, and smart televisions will record viewing history.[25] However, new tests show that even some of these appliances may go further and collect an individual's "ZIP code, phone numbers, date of birth, geolocation, and more through an appliance's smartphone app."[26] Specifically, LG and Samsung collect more personal information than other manufacturers.[27]

II. PRESSING CONSUMER DATA PROTECTION ISSUES

In the world of consumer data protection, the invasiveness of virtual voice assistants and smart doorbell cameras does not go unnoticed. This scrutiny has led to a plethora of lawsuits, as detailed below. The increasing prevalence of technologies that provide convenience and security raise concerns about the extent to which they collect and process personal information. As a result, the trade-off between convenience and data privacy has become a contentious topic in the ongoing debate over how best to balance technological innovation with individual rights and security. Over the past few years, companies that mass-manufacture these devices have paid exorbitant fines due to alleged consumer privacy violations both in the United States and internationally.[28] Government and regulatory bodies around the world

---

[23] Craig Lloyd, *How to Set Up Your Philips Hue Lights*, HOW-TO GEEK (Dec. 19, 2016), https://www.howtogeek.com/247500/how-to-set-up-your-philips-hue-lights/.
[24] *See Privacy Notice*, PHILIPS HUE, https://www.philips-hue.com/en-us/support/legal/privacy-policy (last visited Dec. 17, 2023).
[25] Daniel Wroclawski, *Smart Appliances Promise Convenience and Innovation. But Is Your Privacy Worth the Price?*, CONSUMER REPORTS (Apr. 29, 2023), https://www.consumerreports.org/electronics/privacy/smart-appliances-and-privacy-a1186358482/.
[26] *Id.*
[27] *See id.*
[28] Michael Hill, *The Biggest Data Breach Fines, Penalties, and Settlements So Far*, CSO (Sept. 18, 2023), https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html.

are increasingly scrutinizing the practices of technology companies and emphasizing the need to protect user data and personal information.[29] Whether it is the mishandling of user data, breaches of privacy, or inadequate safeguards against cyber threats, these violations have raised concerns about the balance between technological innovation and individual privacy rights.[30]

On May 31, 2023, the Federal Trade Commission ("FTC") charged Amazon for deceiving the users of its VVA Alexa.[31] In another complaint, the FTC targeted Amazon's SDC, Ring.[32] Multiple lawsuits have been filed against Apple's Siri and Google's Assistant for their privacy infringing properties.[33]

A. The Alexa Complaint and Settlement

As part of a settlement reached with the Department of Justice ("DOJ") and the FTC on July 19, 2023, Amazon agreed to a permanent injunction and a civil penalty.[34] The settlement addressed allegations that Amazon's Alexa VVA violated a U.S. law safeguarding children's privacy, namely the Children's Online Privacy Protection Act ("COPPA").[35]

The DOJ, on behalf of the FTC, filed a complaint on May 31, 2023, asserting that Amazon both hindered parents "from exercising their deletion rights under the COPPA Rule" and retained sensitive voice and geolocation data for extended periods.[36] Amazon allegedly utilized this data for its own business purposes, thereby jeopardizing the security of this information through unwarranted access.[37] According to the complaint, Amazon's actions, including misleading parents, retaining children's data indefinitely, and disregarding deletion requests,

---

[29] *Id.*
[30] *Id.*
[31] *FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests*, FED. TRADE COMM'N (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever [hereinafter FED. TRADE COMM'N].
[32] *See id.*
[33] *See infra* Section II.C.
[34] *See Amazon Agrees to Injunctive Relief and $25 Million Civil Penalty for Alleged Violations of Children's Privacy Law Relating to Alexa*, U.S. DEP'T JUSTICE (July 19, 2023), https://www.justice.gov/opa/pr/amazon-agrees-injunctive-relief-and-25-million-civil-penalty-alleged-violations-childrens [hereinafter Amazon Settlement].
[35] *Id.*
[36] FED. TRADE COMM'N, *supra* note 31.
[37] *Id.*

constituted violations of COPPA and prioritized profit over privacy.[38] Samuel Levine, the Director of the FTC's Bureau of Consumer Protection, emphasized that COPPA prohibits companies from retaining children's data indefinitely for any reason, especially for the purpose of training their algorithms.[39]

The complaint outlined how Amazon led users to believe, including parents, that they could delete voice recordings and geolocation data collected by Alexa.[40] The complaint stated that Amazon failed to fulfill these promises, retained this data for extended durations, and unlawfully used it to improve its Alexa algorithm.[41] Notably, the complaint alleged that Amazon retained children's recordings unless a parent explicitly requested deletion, and even then, it failed to remove all transcripts of children's speech from its databases.[42]

The COPPA Rule mandates that commercial websites or online services directed at children under thirteen-years-old must notify parents about data collection, obtain parental consent, and allow for data deletion upon request.[43] Furthermore, such services must not retain children's data beyond what is reasonably necessary for service provision.[44] Amazon claimed that it retained children's voice recordings to facilitate voice commands, parental review, and the enhancement of Alexa's speech recognition in violation of COPPA and its mandates.[45] However, this unlawful retention allowed Amazon to create a valuable database for training its algorithm to understand children's speech patterns, benefiting the company at the expense of children's privacy.[46]

Accordingly, the U.S. District Court for the Western District of Washington mandated that Amazon was required to pay a $25 million civil fine.[47] The Order enforced injunctive measures, which compelled Amazon to identify and remove dormant child profiles unless specifically

---

[38] *Id.*
[39] *Id.*; COPPA states that "[a]n operator of a Web site or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion." 16 C.F.R. § 312.10.
[40] FED. TRADE COMM'N, *supra* note 31.
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *See* Amazon Settlement, s*upra* note 34.

requested by a parent to retain them.[48] Amazon was also required to inform the parents of children that have accounts of these policy changes.[49] Additionally, the Order forbids Amazon from disseminating misleading information regarding the retention, access, and deletion of geolocation and voice data, including that of children.[50] It further obliges Amazon to erase geolocation data, voice data, and children's personal information upon user or parental request, respectively.[51] Lastly, the Order required Amazon to provide disclosures to consumers concerning its practices related to the retention and deletion of geolocation data and voice information from the Alexa App.[52]

B. The Ring Doorbell Complaint

The FTC has also brought charges against Ring (acquired by Amazon in 2018), alleging a serious breach of its customers' privacy.[53] The FTC contends that Ring allowed many of its employees or contractors to access private videos of consumers, failed to establish essential privacy and security measures, which ultimately enabled hackers to gain control over consumers' accounts, cameras, and video feeds.

As part of a proposed order, (subject to approval by a federal court), Ring will be compelled to erase data derived from videos they inappropriately accessed and implement a comprehensive privacy and security program, which includes new safeguards on the review of videos by human personnel and the enforcement of stringent security controls.[54] These controls encompass the adoption of multi-factor authentication for both employee and customer accounts.[55] Samuel Levine emphasized the importance of privacy and security, stating, "Ring's disregard for privacy and security exposed consumers to spying and harassment . . . The FTC's order makes clear that putting profit over privacy doesn't pay."[56]

---

[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras*, FED. TRADE COMM'N (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users.
[54] *Id.*
[55] *Id.*
[56] *Id.* (quoting Samuel Levine, Director of the FTC's Bureau of Consumer Protection).

According to the FTC's complaint, Ring deceived its customers by failing to restrict employee and contractor access to customers' video content and by using this content for various purposes, including algorithm training, without obtaining proper consent.[57] The complaint outlines the many violations of users' privacy, such as an employee viewing thousands of video recordings of female users over several months, including private spaces in their homes like bathrooms and bedrooms.[58] It took another employee to uncover this misconduct, as Ring had not established monitoring and detection mechanisms for video access.[59] The FTC further claims that Ring did not adequately notify or seek consent from customers for the extensive human review of private video recordings, which was used for various purposes, including algorithm development.[60]

The FTC alleged further that Ring failed to adopt standard security practices to protect consumers from online threats like "credential stuffing" and "brute force" attacks, despite warnings from employees, security experts, and media reports.[61] “Credential stuffing” involves using stolen credentials to access other accounts, while a “brute force” attack is an automated process of repeated password guessing. As a result, hackers continued to exploit vulnerabilities, accessing videos, live streams, and over 55,000 Ring customer account profiles in the United States.[62] Further, these bad actors also changed device settings to access Ring's two-way camera functionality to harass and threaten individuals. The hackers utilized Ring’s functions in numerous ways, such as calling children racial slurs, attempting sexual propositions, and demanding ransoms from families.[63]

The proposed order required Ring to establish a privacy and security program, pay $5.8 million for consumer refunds, and delete customer videos and facial data collected before 2018.[64] It also mandated the reporting of unauthorized access incidents to the FTC and the notification of consumers about the FTC's actions.[65]

As a response to the allegations in both the Alexa and Ring complaints, Amazon stated that while it

---

[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*

> [d]isagree[s] with the FTC's claims regarding both Alexa and Ring, and den[ies] violating the law, these settlements put these matters behind us. Ring promptly addressed the issues at hand on its own years ago, well before the FTC began its inquiry. Our focus has been and remains on delivering products and features our customers love while upholding our commitment to protect their privacy and security.[66]

C. Siri and Google Assistant Lawsuits

Amazon is not the only company under fire for breaches of consumer data protection. On June 29, 2021, U.S. District Judge Beth L. Freeman issued a decision in a class action lawsuit against Google and its parent company Alphabet.[67] The plaintiffs alleged that Google violated California privacy laws and federal privacy laws by "illegally recording and disseminating private conversations of people who accidentally trigger its voice-activated Google Assistant on their smartphones."[68] The plaintiffs alleged that Google unlawfully used their misperceived conversations with Google Assistant for targeted advertising.[69] In response, Google sought dismissal of the claim by asserting that the plaintiffs failed to show that they were harmed by Google Assistant or that Google broke any of its contractual guarantees.[70] Google Spokesman José Castañeda affirmed that the company does not retain consumer audio recordings by default and makes it easy for individuals to manage their privacy preferences.[71]

On July 31, 2021, in another lawsuit, Judge Jeffrey S. White on the U.S. District Court for the Northern District of California ruled that the

---

[66] Adrianne Appel, *FTC Orders Amazon Pay $30M for Alleged Alexa, Ring Privacy Violations*, COMPLIANCE WEEK (June 1, 2023), https://www.complianceweek.com/regulatory-enforcement/ftc-orders-amazon-pay-30m-for-alleged-alexa-ring-privacy-violations/33165.article#toggle (quoting Amazon).

[67] *U.S. Judge Rules Google Must Face Much of Lawsuit over Voice Assistant*, WASH. POST (July 2, 2021), https://www.washingtonpost.com/business/economy/us-judge-rules-google-must-face-much-of-lawsuit-over-voice-assistant/2021/07/02/ff8c3510-db24-11eb-8fb8-aea56b785b00_story.html.

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] Rachel Lerman, *Lawsuits Say Siri and Google Are Listening, Even When They're Not Supposed To*, WASH. POST (Sept. 2, 2021), https://www.washingtonpost.com/technology/2021/09/02/apple-siri-lawsuit-privacy/.

plaintiffs could continue to pursue their claim against Apple's Siri.[72] The plaintiffs alleged that Apple's Siri improperly records private conversations between consumers. They also alleged that the VVA abruptly turns on and violates user privacy by circulating data to third parties.[73] Apple, however, denied the privacy violation allegations by stating that the company does not sell any of its Siri recordings and that the recordings in question cannot be associated with any identifiable individual once stored on its cloud.[74] In its motion to dismiss, Apple emphasized that it believes that privacy is a fundamental human right and "designed Siri so users could enable or disable it at any time."[75]

With the absence of an overarching privacy law that protects consumers from manipulative and deceptive data practices, attorneys seeking to sue technology companies are resorting to sectoral privacy laws. As explained above, these laws offer protection that is limited to specific sectors, making it difficult, and often impossible, to hold the makers of smart home technologies accountable in the consumer privacy world. However, the Fourth Amendment, designed to protect the privacy and security of individuals from unreasonable government intrusion, could provide some protection to consumers.

III. THE FOURTH AMENDMENT, THE THIRD-PARTY DOCTRINE, & TECHNOLOGICAL ADVANCEMENTS

The Fourth Amendment to the United States Constitution states that

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no [w]arrants shall issue but upon probable cause . . . describing the place to be searched, and the . . . things to be seized.[76]

In *Olmstead v. United States*, the Court limited the Fourth Amendment by finding that Fourth Amendment protections did not apply to information obtained by the government in a physical trespass.[77]

---

[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] U.S. CONST. amend. IV.
[77] Olmstead v. United States, 277 U.S. 438, 473–478 (1928).

However, in *Katz v. United States*, the Court overruled *Olmstead*, providing that the Fourth Amendment "protects people, not places."[78] Thus, the Fourth Amendment protects individuals even if there was no physical intrusion.[79] Justice Harlan, concurring, articulated a two-part test (later coined as the *Katz* test).[80] The *Katz* test first asks whether a person exhibited an actual (subjective) expectation of privacy, and second, whether that expectation of privacy was one that society is prepared to recognize as "reasonable" (objective).[81] The *Katz* test has become essential in Fourth Amendment analysis generally. Since the widespread adoption of the *Katz* test, the Court has grappled with what a "reasonable" expectation of privacy looks like in the wake of rapid technological advancements. The Court has gradually adjusted Fourth Amendment protections to balance individual privacy protections with both the government's and society's uses of new technology.

For example, in *Riley v. California*, the Court modified the general rule that searches subsequent to arrest are categorically exempt from the Fourth Amendment's warrant requirement.[82] The Court excluded cell phones from that exception because cell phone searches implicate privacy concerns far beyond those implicated by the search of a cigarette pack, wallet, or purse.[83] This is because, unlike those items, cell phones "place vast quantities of personal information literally in the hands of individuals."[84] In *Kyllo v. United States*, the Court held that police's use of thermal imaging technology constituted a Fourth Amendment search because it provided the government "information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area.'"[85] In *Carpenter v. United States*, the Court considered whether remote location monitoring of Mr. Carpenter's cell phone through cell-site location information ("CSLI") gathered by his wireless carrier constituted a search under the Fourth Amendment.[86] Each time a phone connects to a cell site, it generates a time-stamped record, which is known as CSLI.[87] In recent years, phone companies have begun to collect

---

[78] Katz v. United States, 389 U.S. 347, 351 (1967).
[79] *See id.*
[80] *Id.* at 361.
[81] *Id.*
[82] Riley v. California, 573 U.S. 373, 386 (2014).
[83] *Id.* at 391–98.
[84] *Id.* at 386.
[85] Kyllo v. United States, 533 U.S. 27, 34 (2001) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).
[86] Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).
[87] *Id.*

location information from the transmission of text messages and routine data connections.[88] Accordingly, modern cell phones generate increasingly vast amounts of precise CSLI data.[89] The Court narrowly held that monitoring through CSLI constituted a search under the Fourth Amendment.[90] The Court reasoned that "the retrospective quality of the data here gives police access to a category of information otherwise unknowable."[91] Further, with CSLI data, the government is able to travel back in time to retrace a person's whereabouts for up to five years.[92] Police would not even need to know in advance whether they want to follow a particular individual, or when.[93] The Court concluded by citing Justice Brandeis's famous dissent in *Olmstead*: "the Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the government—to ensure that the 'progress of science' does not erode Fourth Amendment protections."[94]

The Court, in grappling with what constitutes a "reasonable" expectation of privacy, has developed the third-party doctrine.[95] In *United States v. Miller*, the Court held that the Fourth Amendment does not protect information revealed to third parties, even if the information was so revealed, under the understanding that the third party would use it for a limited purpose and also would maintain its privacy.[96] For example, in *Smith v. Maryland*, the Court held that the installation of a "pen register," a device which recorded phone numbers dialed from the defendant's home, did not constitute a Fourth Amendment search.[97] First, the *Smith* Court distinguished the case from *Katz* by noting that a pen register does not acquire the "contents of communications."[98] Then, the Court reasoned that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company since it is through telephone company switching equipment that their calls are completed."[99] Thus, cell phone users voluntarily assume the risk that the numbers they dial are not protected. However, in *Carpenter*, the Court

---

[88] *Id.* at 2212.
[89] *Id.*
[90] *Id.* at 2219.
[91] *Id.* at 2218.
[92] *Id.*
[93] *Id.*
[94] *Id.* at 2223 (citing Olmstead v. United States, 277 U.S. 438, 473–74 (1928)) (Brandeis, J., dissenting).
[95] *See, e.g.*, Hoffa v. United States, 385 U.S. 293 (1966); United States v. Miller, 425 U.S. 435 (1976).
[96] *Miller*, 425 U.S at 443–46.
[97] Smith v. Maryland, 442 U.S. 735, 745–46 (1979).
[98] *Id.* at 741.
[99] *Id.* at 742.

limited the seemingly broad reach of the third-party doctrine.[100] The Court first stated that "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 [today] by wireless carriers."[101] Next, the Court addressed the voluntary assumption of risk in the case at hand and distinguished it from that of the foundational third-party search doctrine cases.[102] The Court reasoned that "carrying [a cell phone] is indispensable to participation in modern society," and a user cannot meaningfully assume the risk of volunteering information to a third party because "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[103] Thus, the Court concluded that cell phone users do not meaningfully consent to the transmission of location data.[104]

Apart from limiting the third-party doctrine, the Court also strengthened Fourth Amendment protections in the face of technological advancements. The Court has long respected the importance of an individual's privacy within a home. In *Silverman v. United States*, the Court wrote that "[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable government intrusion."[105] In *Kyllo v. United States*, the Court rejected the argument that a failure to discern intimate details about the home precluded a Fourth Amendment violation. Justice Scalia wrote for the majority and famously stated that "[i]n the home, our cases show, *all* details are intimate details."[106] In *Collins v. Virginia*, the Court found that a police officer may not enter the curtilage of a home to search a vehicle parked therein.[107] This even includes the use of a police dog to sniff the outside of a home.[108] Thus, with the Fourth Amendment protection of an individual's home in mind, we seem to be at a bit of an impasse. The new plethora of smart home information-grabbing technology[109] has placed the strong home protections under the Fourth Amendment on a collision course with the third-party doctrine.

---

[100] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[101] *Id.* at 2210.
[102] *Id.* at 2217–19.
[103] *Id.* at 2220.
[104] *Id.*
[105] Silverman v. United States, 365 U.S. 505, 511 (1961).
[106] Kyllo v. United States, 533 U.S. 27, 37 (2001) (emphasis added).
[107] Collins v. Virginia, 138 S. Ct. 1663, 1675 (2018).
[108] Florida v. Jardines, 569 U.S. 1, 11–12 (2013).
[109] *See supra* Section I.A.

IV. APPLYING THE FOURTH AMENDMENT TO SMART HOME TECHNOLOGY

The Supreme Court has long been aware of how technological growth may affect privacy rights under the Fourth Amendment. As Justice Brandeis stated in *Olmstead*, "the Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections."[110] In response, the Court has accounted for technological advancements in recent cases dealing with the Fourth Amendment and also specifically the third-party doctrine.[111] While the Court's response has helped navigate technological advances generally, Fourth Amendment jurisprudence has not sufficiently evolved to protect individuals' rights that are implicated in different smart home technologies. Different smart home technologies implicate different expectations of privacy. As a result, not all smart home technologies should give rise to full Fourth Amendment protection.

A. Smart Home Technology is Not a Monolith: A "One Size Fits All" Law (or Doctrine) Will Not Work

When advanced technology made its way into consumers' homes, scholars began to raise questions regarding the intrusive aspect of this *Black Mirror-esque* machinery.[112] In 2023, 63.4 million households in the United States are actively using smart home technologies,[113] and therefore are generating data. Smart data has become valuable to law enforcement for tracking and investigating suspects in pending criminal cases.[114] The revealing power of smart home technologies and the intimate data collected will only continue to grow, as more devices are created and more technologies become interconnected via the IoT.[115] Even though the Fourth Amendment protects "the right of people to be

---

[110] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (citing Olmstead v. United States, 277 U.S. 438, 473–474 (1928)) (Brandeis, J., dissenting).
[111] *See supra* Section III.
[112] Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 547 (2017).
[113] In 2022, 57.5 million households in the United States used smart home technologies. *U.S. Smart Home Statistics* (2018–2027), OBERLO, https://www.oberlo.com/statistics/smart-home-statistics (last visited Nov. 12, 2023) [hereinafter OBERLO].
[114] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1936–40 (2013).
[115] Kelsey Finch & Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581, 1599 (2014).

secure in their . . . houses,"[116] the third-party doctrine may give law enforcement access to data arising from people's private homes through smart data.

The technology used by VVAs, (wake word technology), is highly intrusive. These devices are constantly listening within range of their far-field microphones to detect predefined trigger phrases such as "Hey, Alexa." Although users are able to modify the wake word, they cannot disable the technology altogether. Researchers have found Alexa to be only 94% accurate at detecting speech traffic.[117] In addition, Alexa reliably reacted to eighty-nine different unregistered wake words, with a 100% probability of activation to terms such as "Alissa," "Baranca," "Olexa," "Mixer," and "Electra."[118] Therefore, Alexa frequently records and stores conversations on Amazon's cloud without the user ever prompting it to do so.[119] In addition, VVAs can collect forty-eight different data points ranging from voice recordings, geolocation, purchase history, and information about connected devices linked to the VVA,[120] making VVAs "true data hoarders." The technical nature of the VVA devices and the potential intrusiveness of wake word technology warrants treating their collected data with a heightened privacy standard.

SDC devices have the ability to record both audio and video, making the technology arguably more intrusive than VVAs. SDCs will either record continuously or when motion is detected, depending on the settings of the device.[121] These recorded videos will then be automatically stored on the manufacturer's cloud.[122] In 2020, Strategy Analytics estimated that 42.5 million smart home cameras were shipped

---

[116] *See* U.S. CONST. amend. IV.
[117] Kyle Wiggers, *Researchers Identify Dozens of Words that Accidentally Trigger Amazon Echo Speaker*, VENTUREBEAT (July 6, 2020), https://venturebeat.com/ai/researchers-identify-89-words-that-accidentally-trigger-alexa-to-record/.
[118] *Id.*
[119] VVAs are woken up nineteen times per day, on average. Daniel Bennett, *Alexa, How Often Do You Listen In?*, BBC SCI. FOCUS (Mar. 11, 2020), https://www.sciencefocus.com/future-technology/alexa-how-often-do-you-listen-in/.
[120] Alexa collects thirty-seven out of the forty-eight possible data points. Brianne Sandorf, *Smart Assistant Privacy: What Data is Collected and How Do You Protect Yourself,* REVIEWS.ORG (Apr. 6, 2021), https://www.reviews.org/home-security/smart-assistant-privacy-what-data-is-collected-and-how-to-protect-yourself/.
[121] *Do Home Security Cameras Record All the Time?*, MONTAVUE (Nov. 25, 2022), https://montavue.com/blogs/news/do-home-security-cameras-record-all-the-time.
[122] *Id.*

worldwide.[123] Thus, millions of households expose their family members, neighbors, and visitors to potential digital surveillance. Everyday human interactions are recorded, saved, and stored on a cloud, ready to be collected by law enforcement through a simple subpoena or court order. Without proving probable cause, law enforcement officers are able to access data depicting a user leaving her home, coming back from work, picking up mail, playing with her child on the front porch, or greeting neighbors. Accordingly, SDCs also merit heightened privacy protection. The technology is extremely intrusive to individuals' homes as it produces data that invites law enforcement into the private and intimate lives of users.

The invasive nature of the data collected by VVAs and SDCs is categorically different from the data collected by smart appliances, thermostats, and smart lighting. This data generally does not reveal the users' most intimate conversations and cannot constitute direct evidence on its own. In most cases, data collected by this less-invasive type of smart home technology is for functionality purposes: a smart fridge or thermostat will keep a temperature log, a smart television will keep a viewing history, and smart lighting tracks sleeping habits.[124] On its own, the data's content is unlikely to constitute a basis for incrimination. Although, for example, turning off the light in one's bedroom at 10:00 PM may suggest that the user was home at that specific date and time, this data point alone is only circumstantial evidence in a court of law. Unlike VVAs and SDCs which record users' movements and conversations, most smart home technologies collect data on a precise aspect of a user's routine.[125] Therefore, for these devices, reduced privacy protections with regard to the Fourth Amendment and the third-party doctrine are acceptable.

---

[123] Jack Narcotta, *Smart Home Surveillance Camera Global Market Shares*, STRATEGY ANALYTICS (Apr. 30, 2021), https://www.strategyanalytics.com/access-services/devices/connected-home/smart-home/market-data/report-detail/smart-home-surveillance-camera-global-market-shares-april-2021.

[124] Joe Fassler, *Is Your Smart Fridge Spying On You?*, COUNTER (Mar. 16, 2017), https://thecounter.org/smart-fridge-spying/; Ian Bogost, *Your Smart Thermostat Isn't Here To Help You*, ATLANTIC (Sept. 26, 2022), https://www.theatlantic.com/technology/archive/2022/09/who-controls-smart-thermostat-temperature-nest-ecobee/671559/; Steve Voller, *Internet of Things: The Rise of The Smart Light Bulb*, MDI NETWORKS (Oct. 6, 2017), https://www.mdinetworks.com/article.php?id=77#:~:text=Each%20of%20these%20devices%20will,well%20the%20device%20is%20working.

[125] Salma ElSayed, *Machine Learning In Smart Homes*, MEDIUM (Sept. 3, 2020), https://medium.com/swlh/machine-learning-in-smart-homes-5f39e9600cf0.

B. A New & Nuanced Way Forward

As shown above,[126] certain types of IoT smart home technologies have the capacity to produce data with boundless depth and reach in time. Fourth Amendment protection is thus necessary in those instances–even when it conflicts with the third-party doctrine. In an effort to reconcile the third-party doctrine and Fourth Amendment home protections, it is helpful to begin with the analysis in *Riley* (with *Carpenter* in the backdrop) to create a narrow exception to the third-party doctrine for these technologies. The exception must be narrow and nuanced to account for technology that may only collect non-content account data.

Over time, courts have created exceptions for situations in which law enforcement may bypass the warrant requirement. Some examples of exceptions to the warrant requirement include search incident to arrest,[127] exigent circumstances,[128] border searches,[129] and consent.[130] However, these exceptions to the warrant requirement are not to be applied without restraint. For example, the Court in *Riley* found that the justification for bypassing the warrant requirement in searches incident to arrest was inapplicable when applied to cell phones.[131] Traditionally, the exception was justified by the risk of harm to an officer and destruction of evidence during an arrest, along with a suspect's reduced expectation of privacy incident to arrest.[132] In evaluating the expectation of privacy of a cell phone search, the Court looked to the capabilities of the modern cell phone.[133] The capabilities of a cell phone that were listed by the Court was its immense storage capacity, its ability to collect in one place many distinct types of information, and the pervasive and intimate nature of the type of information stored.[134] Thus, the Court ruled that police must get a warrant before searching a cell phone seized incident to an arrest.[135] In the face of IoT technologies, the Court must also place limits on the third-party doctrine.

The Court has already recognized the shortcomings of the third-party doctrine in *Carpenter* by creating a narrow exception for CSLI

---

[126] *See supra* Section IV.A.
[127] Riley v. California, 573 U.S. 373, 384 (2014).
[128] Mincey v. Arizona, 437 U.S. 385, 386 (1978).
[129] United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013).
[130] United States v. Turner, 169 F.3d 84, 87 (1st Cir. 1999).
[131] *See Riley*, 573 U.S. at 403.
[132] *Id.* at 384–93.
[133] *Id.* at 393.
[134] *Id.* at 393–96.
[135] *Id.* at 403.

data.[136] In doing this, the Court first looked to expectations of privacy. Similar to the reasoning in *Riley*, the Court found that the government's arguments failed to account for the "seismic shifts in digital technology that made possible" the continual tracking of Carpenter's location for a long period of time.[137] Thus, the government may not access long-term CSLI without invading an individual's reasonable expectation of privacy.[138] The Court looked next to the idea of "voluntary exposure" under the third-party doctrine.[139] The Court departed from the presumption in *Smith* by explaining that "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up."[140] Further, "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[141] Thus, the Court concluded that "in no meaningful sense does the user voluntarily 'assume[ ] the risk' of turning over a comprehensive dossier of his physical movements."[142]

Under the framework set out by *Riley* and *Carpenter*, the Fourth Amendment must also provide protection against warrantless searches of smart home technologies like VVAs and SDCs by law enforcement for several reasons. First, the data collected by both VVAs and SDCs clearly implicate privacy interests that far outweigh cell phone and CSLI data. VVAs can record human conversation and store its contents on remote clouds without being instructed to do so by the user.[143] Further, VVAs are considered "data hoarders" as they are able to collect forty-eight different data points, ranging from geolocation to purchase history.[144] SDCs are arguably even more intrusive than VVAs. They can record continuous audio and video which automatically stores on the manufacturer's cloud.[145] Next, VVA and SDC technologies are exponentially past the "vast" capabilities of cell phones that the Court in *Riley* was worried about. While cell phones had a standard capacity of sixteen gigabytes,[146] VVAs and SDCs have limitless capacity on remote clouds. The potentially attainable data is not just text messages and pictures but endless high-quality visual feed of the inside of someone's home. Further, these

---

[136] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).
[137] *Id.*
[138] *Id.*
[139] *Id.* at 2220.
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *See supra* Section IV.A.
[144] *Id.*
[145] *Id.*
[146] *See* Riley v. California, 573 U.S. 373, 393 (2014).

technologies present an extreme imbalance when looking at the "voluntary assumption of risk" rationale under the third-party doctrine. When a customer purchases IoT technology to optimize the safety and convenience within their home, they do not also voluntarily invite law enforcement into the intimate private life within their dwelling. The voluntariness of the disclosure should be directly correlated with the level of sensitivity of the data collected. Disclosure of information is becoming a necessity to participate in modern life. Individuals who employ smart home technology should not compromise their privacy in ways they do not understand.

Finally, as stated *supra*, Fourth Amendment jurisprudence "has drawn a firm line at the entrance to the house."[147] The Supreme Court has consistently held that the home is sacred and at the "core of the Fourth Amendment."[148] Accordingly, VVA and SDC technology is the exact type of scientific advancement the Court must look to protect from Fourth Amendment erosion. An exception to the third-party doctrine must be made for invasive smart home technologies, specifically VVAs and SDCs.

However, this exception for smart home technologies should not and cannot be a "one size fits all" exception to the third-party doctrine. As shown above, the nature of data collected by VVAs and SDCs is categorically different from that collected by smart appliances, thermostats, and smart lighting. Further, the Court in *Carpenter* was careful not to disturb former precedents like *Smith*.[149] Thus, the Fourth Amendment need not protect data from smart appliances, thermostats, and smart lights.

First, smart appliances generally collect data related to the work they are trying to achieve. For example, a smart television will record viewing history, and smart light bulbs may collect data on energy consumption or brightness level.[150] This sort of data seems to be more akin to *Smith's* pen register rather than *Carpenter's* CSLI data.[151] Just as a pen register discloses call history and not any communication between the caller and the recipient, TV viewing history and brightness level data does not provide the communications inside an individual's home.[152] Smart appliance data does not "hear sound" like a recorded conversation from a phone call or video footage from SDC technology.[153] *Smith* also

---

[147] *See* Payton v. New York, 445 U.S. 573, 590 (1980).
[148] Wilson v. Layne, 526 U.S. 603, 612 (1999).
[149] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
[150] *See supra* Section I.B.
[151] Smith v. Maryland, 442 U.S. 735, 736 (1979); *Carpenter*, 138 S. Ct. at 2220.
[152] *Id.* at 742.
[153] *Id.* at 741.

addressed the fact that the defendant's telephone was used in his house, where the Supreme Court has consistently held the home at the "core of the Fourth Amendment."[154] *Smith* reasoned that although the "conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed."[155] Further, "[r]egardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete the call."[156] Similar to *Smith*, while individuals must be able to keep the intimate details within their homes private, non-content information like energy consumption or connectivity status does not have an objective or subjective expectation of privacy.

This does not mean that smart appliances, thermostats, and smart lighting are categorically exempt from Fourth Amendment protection like pen registers or bank records. For example, in *Naperville Smart Meter Awareness v. City of Naperville*, the city installed meters that collected residents' energy-usage data at fifteen-minute intervals and stored that data for up to three years.[157] While the Seventh Circuit noted that "an inference cannot be a search," energy-usage data collected at fifteen-minute intervals for three years could reveal details that would be otherwise unavailable to government officials with a physical search.[158] Similarly, the court in *State v. Jones* found that using a pole camera to surveil the defendant's activities outside his residence 24/7 for two months constituted a search under the Fourth Amendment.[159] The court reasoned that "long-term video surveillance will necessarily include a mosaic of intimate details of a person's private life and associations."[160] Thus, when determining whether privacy protections apply to specific smart home technologies, a court must consider the invasiveness of the smart data collected and the behavioral patterns revealed about the user through the data, in which length of time is factored.

When it comes to smart home technology, there should not and cannot be a "one size fits all" exception to the third-party doctrine. The invasive nature of the data collected by VVAs and SDCs is categorically different from the data collected by smart appliances, thermostats, and

---

[154] *Id.* at 743–44; *see also* Wilson v. Layne, 526 U.S. 603, 612 (1999).
[155] *Id.* at 743.
[156] *Id.*
[157] Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521 (7th Cir. 2018).
[158] *Id.* at 526.
[159] State v. Jones, 903 N.W.2d 101 (S.D. 2017).
[160] *Id.* at 110.

smart lighting. Accordingly, the Fourth Amendment must protect against smart technologies like VVAs and SDCs, but not necessarily smart appliances, smart light bulbs, and thermostats.

CONCLUSION

The sanctity of the home in Fourth Amendment jurisprudence has never been questioned. The Supreme Court in *Miller v. United States* quoted William Pitt's address to the House of the Commons in 1763, where he proclaimed:

> [t]he poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England cannot enter—all his force dares not cross the threshold of the ruined tenement![161]

The spirit of William Pitt's address is still generally accepted today. However, what a home looked like in 1763 is much different than what a home looks like today, in 2023. In 2023, 63.4 million households in the United States actively use smart home technologies.[162] Smart home devices disseminate a plethora of constant, intimate, and revealing data. However, each smart device is unique. The underlying architecture differs from one apparatus to another, and the privacy challenges are therefore unique to each device. Further, while these devices have great potential to optimize security, convenience, and energy conversion, they also put their users at risk. Specifically, the third-party doctrine holds that individuals have no expectation of privacy regarding information disclosed to third parties, notably to service providers.[163] On that account, smart home technology has set the Fourth Amendment on a crash course with the third-party doctrine.

Accordingly, the Court must, as it's done before, stretch the interpretation of the Fourth Amendment to protect against new technological advances in the American home. But the plethora of smart home technology requires a deeper look. While SDC and VVA technology may need categorical Fourth Amendment protection, smart appliances,

---

[161] Miller v. United States, 357 U.S. 301, 307 (1958) (quoting William Pitt, Earl of Chatham).
[162] OBERLO, *supra* note 113.
[163] *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

thermostats, and lights do not. Depending on the length of time and behavioral patterns revealed about the individual through the smart appliances, thermostats, and lights, the data collected may be more akin to the pen register in *Smith* rather than the CSLI data in *Carpenter*. Thus, smart appliances, lights, and thermostats should not be afforded the same Fourth Amendment protections as VVA and SDC technology.

Smart home technology has put Fourth Amendment jurisprudence on a junction that demands course-correction. The vast and intimate nature of smart home data is overdue for the Supreme Court's consideration. The Court must use this opportunity to provide an intricate solution that protects individuals' home privacy while also preventing law enforcement from side-stepping Fourth Amendment protections with the third-party doctrine.