TOURO COLLEGE
JACOB D. FUCHSBERG LAW CENTER
Where Knowledge and Values Meet

Touro Law Review

Volume 36 | Number 2 Article 12

2020

A New Era: Digital Curtilage and Alexa-Enabled Smart Home Devices

Johanna Sanchez
Touro Law Center

A NEW ERA: DIGITAL CURTILAGE AND ALEXA-ENABLED SMART HOME DEVICES

Johanna Sanchez[*]

[*]Touro College Jacob D. Fuchsberg Law Center, J.D., 2020; John Jay College of Criminal Justice, B.A. in Philosophy, Certificate in Dispute and Resolutions, 2016. I would like to give a special thanks to my Dad, Daniel, for his unconditional love and encouragement in everything I do. My Dad is a strong pillar of wisdom and power in my life. I would also like to thank my partner, William, for his immeasurable love and support, especially throughout these last two years as I pursued my Juris Doctor degree. I would also like to thank my family for their love and enthusiasm, and my biological father, Leo, who I know is proudly watching over me. Next, thank you to Editor-in-Chief, Nicholas Maggio, for his guidance throughout the editing process. Lastly, many thanks to my faculty advisor, Professor Mark Cohen, for his assistance in providing extensive feedback throughout the writing process.

I. INTRODUCTION

Amazon designed the virtual personal assistant, Alexa, and programmed the virtual assistant in millions of Alexa-enabled devices, creating a large class of smart devices that now reside in American homes and offices.[1] However, any convenience gained from Alexa-enabled devices, such as Amazon's Echo device, creates significant privacy concerns. Engagement with an Alexa-enabled smart home device puts the user at risk of exposing personal and incriminating data to law enforcement even before they obtain a search warrant based on probable cause. Of significant concern is that the Supreme Court of the United States has not ruled on whether it is constitutional for law enforcement to obtain Alexa-enabled smart home data without a warrant supported by probable cause.

Recently, law enforcement used the recordings from Alexa-enabled smart home devices in at least three criminal case investigations. A judge in New Hampshire ordered Amazon to release recordings from an Alexa-enabled Echo device located in a home

[1] Ben Fox Rubin, *Amazon sees Alexa Devices More Than Double in Just One Year*, C|NET (Jan. 6, 2020, 6:00 a.m.), https://www.cnet.com/news/amazon-sees-alexa-devices-more-than-double-in-just-one-year/.

where two women were fatally stabbed.[2] In a similar case, the defendant, under criminal investigation, voluntarily gave up the recordings from the Alexa-enabled Echo device.[3] In other situations, law enforcement obtained warrants for the recordings from Alexa-enabled Echo devices located in homes.[4] While the government's use of Alexa-enabled smart home data in criminal prosecution proceedings is not yet prevalent, the use of this data without constitutional restraints poses significant privacy concerns.

The framers of the United States Constitution did not have reason to develop law concerning the government's use of smart technology to acquire, store, and analyze personal information about Americans.[5] When the founding fathers drafted and ratified the Constitution, there were no electronic devices such as satellites, digital cameras, and computers. Today, Global Positioning Systems (GPS) provide the velocity, location, and time of cars and airplanes.[6] A Ford Motor representative stated, "[w]e know everyone who breaks the law. We know when you're doing it. We have GPS in your car, so we know what you're doing."[7] Recently, the Supreme Court recognized the growth of cellphone use by stating, "[t]here are 396 million cell phone service accounts in the United States . . . for a Nation of 326 million people."[8] Furthermore, the current Alexa-enabled smart home devices transmit data displaying continuous and intimate patterns of users' routines, habits, thoughts, and other daily life activities. Thus,

---

[2] Debra Cassens Weiss, *Judge Orders Amazon to Provide Echo recordings in Double Homicide Case*, ABA J. (Nov. 12, 2018), http://www.abajournal.com/news/article/judge_orders_amazon_to_provide_echo_recordings_in_double_homicide_case.

[3] *Id.*

[4] Kayla Epstein, *Police Think Amazon's Alexa May Have Information on a Fatal Stabbing Case*, THE WASH. POST (Nov. 2, 2019), https://www.washingtonpost.com/technology/2019/11/02/police-think-amazons-alexa-may-have-information-fatal-stabbing-case/.

[5] *See* Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 IDAHO L. REV. 639, 641 (2015) ("These devices will send data from the device in the home out to the cloud, leaving their private nature uncertain, and many others will be designed to operate outside the home, like driverless cars, wearables, and smart retailers.").

[6] *What is GPS and How Does it Work?*, MEDALLION GPS (Jul. 19, 2018), https://medalliongps.com/blogs/medallion-car-tracking-and-protection/what-is-gps-and-how-does-it-work.

[7] Stephen E. Henderson, *Our Records Panopticon and the American Bar Association Standards for Criminal Justice*, 66 OKLA. L. REV. 699, 705 (2014).

[8] Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

technology has rapidly advanced since the enactment of the Constitution.

Law enforcement's unchecked access to Alexa-enabled smart home devices contravenes the framers' intent to protect Americans from unreasonable governmental searches and seizures, notably within one's home. The Fourth Amendment of the United States Constitution is a response to the "'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[9] As a result, the framers of the Constitution created specific guidelines to administer search warrants in the United States.

Contrary to England's "colonial writs of assistance,"[10] the Fourth Amendment requires specificity to execute search warrants. Alexa-enabled smart home devices continue to grow in sophistication, and whether law enforcement's use of this data is constitutional requires an examination of the Fourth Amendment.

This Note addresses how the Fourth Amendment should protect data collected from Alexa-enabled smart home devices against unlawful governmental search and seizure. Specifically, this Note analyzes Supreme Court cases discussing technological advancements and demonstrates how current federal law can protect Alexa-enabled smart home devices. This Note also demonstrates how redefining the Fourth Amendment's term "effects" can expand its scope to protect Alexa-enabled smart home devices and the data they radiate. Also, this Note analyzes Andrew Ferguson's theory of digital curtilage[11] and shows how this new framework can be used by judges to protect the data collected from Alexa-enabled smart home devices.

This Note is divided into seven parts. Part II of this Note discusses the societal benefits derived from the Alexa-enabled smart home device. Part III focuses exclusively on Supreme Court cases regarding the Fourth Amendment and its application towards different electronic devices. Part IV demonstrates how current federal law can protect Alexa-enabled smart home devices from unreasonable searches or seizures. Part V shows how redefining the Fourth Amendment's term "effect" can expand its scope to protect Alexa-enabled smart devices. Part VI presents the theory of "digital curtilage" and discusses

---

[9] Riley v. California, 573 U.S. 373, 403 (2014).

[10] *Id.*

[11] Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 809 (2016).

how this new framework can protect Alexa-enabled smart devices and the data they radiate. Lastly, Part VII concludes with a summary of the methods used in this Note to protect Alexa-enabled smart home devices from unlawful government intrusion.

II. SOCIETY'S BENEFITS DERIVED FROM THE ALEXA-ENABLED SMART HOME DEVICE

A. A New Form of Electronic Surveillance

1. What is a smart device?

At this rate, any tangible property can become *smart* by merely adding sensors, and "a tiny bit of computing capabilities and network connectivity."[12] Amazon's Alexa-enabled home device falls under a category of smart devices. A smart device is "a context-aware electronic device capable of performing autonomous computing and connecting to other devices…wirelessly for data exchange."[13] Smart devices possess features of "context-awareness, autonomous computing, and connectivity."[14] Context-awareness is "the ability of a system . . . to gather information about its environment at any given time and adapt behaviors accordingly."[15] Autonomous computing is a device's ability to "perform[sic] tasks autonomously without the direct command of the user."[16] The connectivity feature refers to a smart device's ability to connect wirelessly to a data network and cloud system.[17] The cloud stores data on an offsite location:

> [The cloud is an] internet data center where software and services reside, instead of being stored on local hardware such as your computer or other electronic devices. Cloud computing harnesses the power of the internet to outsource tasks, such as housing software or file storage. Cloud storage refers to the process of saving data to an offsite storage system not found on

---

[12] Manuel Silverio, *What is a Smart Device?- The Key Concept of the Internet of Things*, MEDIUM (Dec. 29, 2019), https://towardsdatascience.com/what-is-a-smart-device-the-key-concept-of-the-internet-of-things-52da69f6f91b.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

> your electronic device. This isn't saving items to a folder on your desktop or transferring items onto a thumb drive. Cloud storage systems are maintained by a third party, and you save your files to a remote database thanks to the power of the internet. This allows you to backup and access your files from any device that is connected to the internet.[18]

As an alternative to buying external hard drives, cloud storage is convenient and cost-effective.

2. What is a voice recognition device?

Voice recognition is "the technology by which sounds, words or phrases spoken by humans are converted into electrical signals, and these signals are transformed into coding patterns to which meaning has been assigned."[19] Voice recognition technology created a voice assistant industry where software developers use artificial intelligence and machine learning capabilities to improve their voice recognition devices.

Voice recognition devices have evolved throughout the years and continue to evolve as devices need updating.[20] In 1961, IBM introduced the IBM Shoebox as the first digital speech recognition technology, recognizing 16 words.[21] In 2011, Apple introduced Siri.[22] In 2013, Microsoft introduced Cortana.[23] In 2014, Amazon introduced

---

[18] *What is Cloud Storage and How Does it Work?*, CDW (Jan. 8, 2019), https://www.cdw.com/content/cdw/en/articles/cloud/2019/01/08/what-is-cloud-storage.html?gclid=EAIaIQobChMIw_e78-Ht5wIVj5OzCh35dgA0EAAYAiAAEgJMLvD_BwE&cm_ven=acquirgy&cm_cat=google&cm_pla=SEO+Articles&cm_ite=Cloud+Storage+Definition+E&ef_id=EAIaIQobChMIw_e78-Ht5wIVj5OzCh35dgA0EAAYAiAAEgJMLvD_BwE:G:s&s_kwcid=AL!4223!3!395466473699!e!!g!!what%20is%20cloud%20storage&s_kwcid=AL!4223!3!395466473699!e!!g!!what%20is%20cloud%20storage.

[19] Jim Baumann, *Voice Recognition*, HUMAN INTERFACE TECHNOLOGY LABORATORY, http://www.hitl.washington.edu/projects/knowledge_base/virtual-worlds/EVE/I.D.2.d.VoiceRecognition.html (last visited Jan. 15, 2020).

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.*

Alexa.[24] In 2017, Google launched Google Home with multi-user support to recognize six different voices.[25]

Amazon created Alexa, an artificial intelligence system, to engage and understand humans.[26] The Alexa-enabled Echo device is a smart home device that features voice recognition. The ability to engage and understand humans requires smart devices to learn about its user's likes and dislikes, habits, and much more.

3. The Alexa-enabled Echo device assists law enforcement

Richard Clarke created the expression "dataveillance to define the systematic observation, collation, and dissemination that modern computing make[s] possible."[27] Smart devices possess an ever-increasing capacity to record intimate information by "the combined impact of an increased ability to collect[,] process[,] and disseminate information."[28] By design, smart home devices also gather sensitive information about their owner and store it in the cloud system.[29] Amazon's Alexa-enabled Echo device continuously records and collects data about the user's life to produce efficient and convenient virtual assistance.[30]

The Alexa-enabled Echo device also creates the potential for law enforcement to obtain this accumulation of information and use it against the user. For example, a judge in New Hampshire ordered Amazon to release recordings from an Echo device during a criminal investigation.[31] Amazon's Alexa-enabled Echo device activates with the wake word Alexa when it begins to record and save the data collected.[32] Considering the smart home device's capacity to store incriminating information, gaining access to the data collected appeared pertinent to the investigation. Prosecutors reasoned that the

---

[24] *Id.*

[25] *Id.*

[26] George Anders, *"Alexa, Understand Me"*, MIT TECH. REV. (Aug. 9, 2017), https://www.technologyreview.com/s/608571/alexa-understand-me/.

[27] M. Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 PENN ST. L. REV. 809, 822 (2010).

[28] *Id.*

[29] *The Mystery of the Amazon Echo Data*, PRIVACY INTERNATIONAL (Apr. 17, 2019), https://privacyinternational.org/news-analysis/2819/mystery-amazon-echo-data.

[30] *Id.*

[31] Weiss, *supra* note 2.

[32] *Id.*

Echo device could have activated at the time of the crime.[33] However, an Amazon spokesperson said, "no information [would] be released until the company [was] served with a valid legal demand."[34] This case demonstrates law enforcement's growing interest in obtaining the data collected from the Alexa-enabled smart home device.

Moreover, in a similar case, a prosecutor sought the recordings from the defendant's Alexa-enabled Echo smart speaker as evidence in a criminal investigation.[35] Since Amazon's Echo device works by endlessly listening for the wake word Alexa, the device records the voice of the user even without his knowledge. Hence, the voice-activated Echo device could potentially provide information about the incident.[36] Amazon's lawyers wrote a memo seeking to quash the prosecutor's request for a search warrant by arguing that the First Amendment protected the recorded speech.[37] Subsequently, the defendant voluntarily gave up the recordings from his Alexa-enabled smart device, which led Amazon to provide prosecutors with the recorded data.[38] This scenario demonstrates that when a user of Amazon's Alexa-enabled smart home device voluntarily consents to share the information gathered by the smart device, he waives his privacy rights.

Recently, Amazon commented on its compliance with the governmental demands of the Alexa-enabled Echo smart device.[39] Turning over the data to law enforcement depends on whether the government provides a lawful court order requiring the disclosure.[40] In 2019, police obtained a warrant for the recordings from Alexa-enabled Echo devices that were in a house during the time a murder ensued.[41] In justifying the probable cause standard for the execution of a warrant, police officers wrote, "[i]t is believed that evidence of crimes, audio recordings capturing the attack on victim Silvia Crespo that occurred in the main bedroom … may be found on the server maintained by or for Amazon."[42]

---

[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] Epstein, *supra* note 4.
[40] *Id.*
[41] *Id.*
[42] *Id.*

In reply, an Amazon representative stated, "…the company does not disclose customer information in response to government demands unless we're required to do so to comply with a legally valid and binding order[;] the company objects to overbroad or otherwise inappropriate demands as a matter of course."[43] However, a spokesman for the Hallandale Beach Police Department later stated, "we did receive [the Alexa-enabled Echo device] recordings, and we are in the process of analyzing the information that was sent to us."[44] It appears from this case that Amazon believes in both the spirit of the Fourth Amendment and its text when asked by the government to disclose the data collected from Alexa-enabled smart home devices.

A District Court also followed the spirit of the Fourth Amendment and its text regarding the disclosure of data collected from Alexa-enabled smart home devices in *United States v. Chiu.*[45] Chiu, the defendant, moved to suppress the evidence seized from his residence, conducted according to a warrant.[46] The evidence seized included an Alexa-enabled Echo device that officers believed contained child pornography.[47] The court denied the motion to suppress the evidence because "the search warrant affidavit provided probable cause that evidence of a crime, particularly possession or receipt of child pornography, would be found in Chiu's residence."[48]

Moreover, the state court considered the officer's expertise in knowing the habits of child pornography consumers for the issuance of a search warrant.[49] Child pornography consumers "maintain their digital or electronic collections in a safe, secure, and private environment . . . kept close by . . . to enable the individual to view or access the material, and to safeguard it."[50] Considering this information, the judge denied Chiu's motion to suppress.[51] This case shows how some courts apply the Fourth Amendment to protect Alexa-enabled smart home devices and the data it stores. Since the Supreme Court has not decided on Fourth Amendment issues concerning Alexa-

---

[43] *Id.*

[44] *Id.*

[45] United States v. Chiu, No. CR 18-10431-DJC, 2019 WL 3755953, at *1 (D. Mass. Aug. 8, 2019).

[46] *Id.*

[47] *Id*. at 2*.

[48] *Id*. at 3*.

[49] *Id.*

[50] *Id*.

[51] *Id*. at 4*.

enabled smart home devices, lower courts create inconsistent results regarding smart home devices and governmental searches and seizures.

As provided by law, securing a search warrant requires law enforcement to obtain a written order signed by a court authorizing the officer to conduct a search or seizure. Warrants are precise and authorize law enforcement officers to search in particular locations and seize specific items. Governmental searches and seizures performed without a valid warrant are deemed presumptively invalid.[52] Courts generally suppress evidence obtained from governmental searches and seizure conducted without a warrant unless a court finds that the search was reasonable under the circumstances.[53]

4. Electronic devices improve law enforcement investigations

Consumers' use of smart home devices leaves behind a digital footprint that can be utilized in government investigations as police recognize the value of digital surveillance.[54] In the past, evidence at a crime scene included blood, fingerprints, footmarks, fabric from a shirt, and hair. However, technological advancements created virtual evidence that derives from computers, cell phones, watches, and more. For instance, law enforcement officials use the data collected from Fitbits[55] activity trackers to Ring[56] doorbells for help in their

---

[52] Carroll v. United States, 267 U.S. 132, 147-48 (1925).

[53] *Id.* at 149:

> If the search and seizure without a warrant are made upon probable cause, that is, upon a belief, reasonably arising out of circumstances known to the seizing officer, that an automobile or other vehicle contains that which by law is subject to seizure and destruction, the search and seizure are valid. The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens.

Id.

[54] Epstein, *supra* note 4.

[55] *Fitbit Privacy Policy*, FITBIT, https://www.fitbit.com/us/legal/privacy-policy (Effective Dec. 18, 2019) (explaining Fitbit's ability to collect data to estimate a variety of metrics like the number of steps users take, their distance traveled, calories burned, heart rate, sleep stages, and location. When a user's Fitbit syncs with Fitbit's applications and software, the data recorded from the user's Fitbit is transferred to Fitbit's servers.).

[56] Amanda Derrick, *What is the Ring Doorbell and How Does it Work?*, LIFEWIRE (May 8, 2020), https://www.lifewire.com/how-ring-doorbell-works-4583925 (explaining how Ring

investigations.[57] Officers might use a Fitbit to discredit a suspect's alibi by using the Fitbit data to show he was out walking instead of sleeping.

Moreover, Ring openly partnered with police and "allows law enforcement to access the camera feeds captured and transmitted by their devices."[58] The camera footage from Ring doorbells can create a new kind of neighborhood watch. However, "Ring does not disclose customer information in response to government demands unless [it is] required to do so to comply with a legally valid and binding order."[59] Like Amazon, Ring requires law enforcement to obtain a search warrant based on probable cause to access the footage from its device.

Additionally, law enforcement officers use Live Scan,[60] which captures fingerprints electronically and checks the marks against a national database.[61] Live Scan then alerts law enforcement officers to suspects that have provided false identification information.[62] Live Scan helps officers collect accurate information about a person's past encounter with law enforcement and biographic information.

Law enforcement officers are interested in digital surveillance because physical location and time, among other information, are essential in investigating a crime.[63] Smart devices can identify suspects near a crime scene through geolocation information, which can result in the discredit of a suspect's recollection of facts.[64] The use

---

doorbells detect and capture video of motion, which instantly sends a push notification to the user's device and stores the footage in the cloud with a subscription).

[57] Epstein, *supra* note 54.

[58] *Id.*

[59] Drew Harwell, *Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns*, THE WASH. POST (Aug. 28, 2019), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/?arc404=true.

[60] *What is Electronic "Live Scan" Fingerprinting Technology?*, ACCURATE BIOMETRICS, https://accuratebiometrics.com/what-is-livescan (last visited May 23, 2020) (describing Live Scan as an electronic means of capturing fingerprints in a digitized format, which transmit the data to a state repository or the FBI to be searched against criminal databases. By processing fingerprints electronically, a person's criminal history background can be provided within a matter of hours.).

[61] Julie Mennell & Ian Shaw, *Science and Technology at the Crime Scene*, MEASUREMENT CONTROL (Apr. 2005), https://journals.sagepub.com/doi/pdf/10.1177/002029400503800301.

[62] *Id.*

[63] *Id*.

[64] *Forensic Analysis of Mobile Malware*, SCIENCEDIRECT https://www.sciencedirect.com/topics/computer-science/mobile-device-forensics (last visited Jan. 1, 2020).

of technological devices for investigation purposes will continue to increase as technology becomes more pervasive in society.

Amazon's most recent information request report, which covers July 2019 through December 2019, demonstrates that the company received 1,841 subpoenas and 440 search warrants and turned over some or all of the information requested.[65] Alex Ferguson considered the danger of obtaining a user's Alexa-enabled smart home devices:

> Because Alexa is only supposed to activate and record when given a specific voice command, it was unclear whether obtaining a blanket warrant to examine a device's transmissions could amount to a "fishing expedition." We live in a world where we have these little digital spies listening to us in our homes, in our cars, and in our phones. It is going to become pretty commonplace that law enforcement is going to request as much digital evidence as they can about us using the legal means available. We have really created a privacy-invasive world because of consumer convenience.[66]

Thus, although smart home devices benefit consumers, they may also be abused by law enforcement.

B. Amazon's Alexa Proves Beneficial to Consumers

In-home connectivity has become a significant selling point for homeowners. Amazon designed the voice-controlled personal assistant "Alexa" to serve as the control center to transform homes into smart homes. The Alexa-enabled smart home device, Echo, is a speaker powered by cloud-based software that allows users to query "Alexa" to perform tasks, obtain information, and control other in-home smart devices. Since Alexa is a virtual assistant, just as any assistant, the information received is *recorded*. Consequently, Alexa-enabled devices record and collect information that viewed together can reveal an enormous amount of detailed information about the user.

As a virtual assistant, Alexa becomes more efficient when connected to other smart devices. For example, smart lighting lets

---

[65] AMAZON INFORMATION REQUEST REPORT https://d1.awsstatic.com/certifications/Information_Request_Report_December_2019.pdf.

[66] Epstein, *supra* note 4.

users control connected lights by voice when paired with Alexa.[67] Smart plugs also help users turn their everyday appliances into part of their smart home.[68] By using smart plugs and connecting them with Alexa, users can "keep track of [their] electricity consumption with an energy-monitoring smart plug."[69] Users can also keep an eye on their homes by connecting smart cameras to Alexa. By pairing these devices, users can instantly monitor the inside and outside of their homes from work.[70]

Alexa personalizes its contents for each user by recognizing a user's unique voice, which allows the device to personalize the content shown.[71] The smart home device connects users to their personalized choice of entertainment. For instance, Alexa can individualize a user's daily news updates. Users can also create routines using Alexa to synchronize their habits with Alexa's actions.[72] A routine is Alexa's ability to perform a series of actions with a single command.[73] For example, a user can say, "Alexa, start my day" so that Alexa responds by announcing the weather forecast, turning on the kitchen lights, and reading the news out loud.[74]

Alexa, as a virtual assistant, keeps users organized and prepared for their daily activities. Alexa can access a user's "calendar or email from Google, G Suite, iCloud, Outlook.com, or Office 365,"[75] and the user can ask Alexa to add events to his calendar. Without touching any device, users can go through a day's worth of emails

---

[67] *Alexa Features: Smart Home*, AMAZON, https://www.amazon.com/b/ref=aeg_lp_sh_d/ref=s9_acss_bw_cg_aegflp_4b1_w?node=17934679011&pf_rd_m=ATVPDKIKX0DER&pf_rd_s=merchandised-search-6&pf_rd_r=YF0Q1SMNDWYXBCKDRQYN&pf_rd_t=101&pf_rd_p=13955371-8a01-4a1a-8e17-c735780ef269&pf_rd_i=17934672011 (last visited Jan. 2, 2020).

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] *Alexa Features: News & Information*, AMAZON, https://www.amazon.com/b/ref=aeg_lp_ni_d_text/ref=s9_acss_bw_cg_aegflp_md1_w?node=17934677011&pf_rd_m=ATVPDKIKX0DER&pf_rd_s=merchandised-search-6&pf_rd_r=YF0Q1SMNDWYXBCKDRQYN&pf_rd_t=101&pf_rd_p=13955371-8a01-4a1a-8e17-c735780ef269&pf_rd_i=17934672011 (last visited Jan. 2, 2020).

[72] *Alexa Features: Smart Home*, *supra* note 67.

[73] *Id.*

[74] *Id.*

[75] *Alexa Features: Productivity*, AMAZON, https://www.amazon.com/b/ref=aeg_lp_prod_d_text/ref=s9_acss_bw_cg_aegflp_md1_w?node=17934678011&pf_rd_m=ATVPDKIKX0DER&pf_rd_s=merchandised-search-6&pf_rd_r=YF0Q1SMNDWYXBCKDRQYN&pf_rd_t=101&pf_rd_p=13955371-8a01-4a1a-8e17-c735780ef269&pf_rd_i=17934672011 (last visited Jan. 2, 2020).

before their coffee is ready because Alexa can even read the user's emails out loud.[76] Alexa also tells users the traffic conditions and informs users about the duration of their commute.[77] Alexa further enables users to communicate with others outside the home in over 150 countries worldwide.[78]

A significant development in the Alexa-enabled smart home device is its ability to handle and access health information. Amazon created a way for companies to transmit information like medical diagnosis and pharmaceutical prescriptions via Alexa while remaining Health Insurance Portability and Accountability Act (HIPAA) compliant.[79] Amazon invited health care companies to develop voice programs which Amazon refers to as "skills."[80] The head of Alexa Heath and Wellness stated, "[t]hese new skills are designed to help customers manage a variety of healthcare needs at home [by] simply using voice . . . whether it's booking a medical appointment, accessing hospital post-discharge instructions, checking on the status of a prescription delivery, and more."[81]

Recently, the Mayo Clinic launched a new "skill" for Alexa-enabled smart home devices to conveniently inform users of newly developed information about the COVID-19 pandemic.[82] When users enable the Mayo Clinic Answers on the COVID-19 skill, they can receive information from the Centers for Disease Control and Prevention and Mayo Clinic experts.[83] A Mayo Clinic physician stated the new skill "offers the latest information on symptoms, prevention [,]and how to cope in a hands-free way using only the voice – a fact that is especially important when we're trying to reduce the spread of

---

[76] *Id.*

[77] *Alexa Features: News & Information*, *supra* note 71.

[78] *Alexa Features: Communication*, AMAZON, https://www.amazon.com/b/ref=aeg_flp_ent_text/ref=s9_acss_bw_cg_aegflp_md1_w?node=17934681011&pf_rd_m=ATVPDKIKX0DER&pf_rd_s=merchandised-search-6&pf_rd_r=YF0Q1SMNDWYXBCKDRQYN&pf_rd_t=101&pf_rd_p=13955371-8a01-4a1a-8e17-c735780ef269&pf_rd_i=17934672011 (last visited Jan. 2, 2020).

[79] Angela Chen, *Amazon's Alexa Now Handles Patient Health Information*, THE VERGE, (Apr. 4, 2019), https://www.theverge.com/2019/4/4/18295260/amazon-hipaa-alexa-echo-patient-health-information-privacy-voice-assistant.

[80] *Id.*

[81] *Id.*

[82] *Coronavirus Updates: Mayo Clinic Launches New Covid-19 Information Skill For Amazon's* Alexa, CBS MINNESOTA, (Apr. 27, 2020), https://minnesota.cbslocal.com/2020/04/27/coronavirus-updates-mayo-clinic-launches-new-covid-19-information-skill-for-amazons-alexa/.

[83] *Id.*

the virus transmitted by physical contact."[84] Consequently, Alexa-enabled devices record and collect information that viewed together can reveal an enormous amount of detailed information about the user.

III. THE FOURTH AMENDMENT AND ELECTRONIC DEVICES

The Supreme Court regularly addresses advances in modern technology and, when necessary, enlarges the Fourth Amendment's protection.[85] The Fourth Amendment protects against unreasonable searches and seizures to prevent officials from arbitrary and oppressive interference with an individual's privacy.[86] Search and seizure are essential terms of art in the Fourth Amendment because they are threshold elements to determine whether law enforcement's action constitutes a violation of the law. According to previous Supreme Court case law, the location and classification of an electronic device are fundamental in determining whether law enforcement committed a Fourth Amendment search.[87] For many years, courts have adjudicated matters about data stored on electronic devices.[88] However, the Court has not addressed data collected and recorded by Alexa-enabled smart home devices.

A. 1928: Wiretap

Olmstead v. United States[89] concerned the applicability of the Fourth Amendment to warrantless wiretapping by government agents.

---

[84] *Id.*

[85] *See* Marjorie A. Shields, *Fourth Amendment Protections, and Equivalent State Constitutional Protections, as Applied to the Use of GPS Technology, Transponder, or the Like, to Monitor Location and Movement of Motor Vehicle, Aircraft, or Watercraft,* 5 A.L.R. 6th 385 (Originally published in 2005).

[86] U.S. CONST. amend. IV; United States v. Martinez-Fuerte, 428 U.S. 543, 554 (1976).

[87] *See* James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317 (2002).

[88] *See, e.g.*, Riley v. California, 573 U.S. 373, 378-79 (2014) (smartphones); United States v. Warchak, 631 F.3d 266, 288 (6th Cir. 2010) (email); United States v. Romm, 455 F.3d 990, 994 (9th Cir. 2006) (laptop); United States v. Carey, 172 F.3d 1268, 1270 (10th Cir. 1999) (computer); United States v. Barth. 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) (holding that the "Fourth Amendment protection of closed computer files and hard drives is similar to the protection it affords a person's closed containers and closed personal effects."); *See generally* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531,542 (2005) (noting that computers store "a tremendous amount of information that most users do not know about and cannot control.").

[89] *See* Olmstead v. United States, 277 U.S. 438 (1928).

Here, federal officers used wiretaps to intercept Olmstead's telephone conversations.[90] The Court reasoned that the Fourth Amendment protects houses and offices from which the conversations arose against unreasonable searches and seizures, but only from physical trespasses.[91] The Court determined that officers secured the evidence solely by using their sense of hearing.[92] The Court did not consider wiretaps, used to listen to Olmstead's conversations, as a physical trespass because officers installed the wiretaps on telephone lines *outside* Olmstead's property.[93] The Court stated, "the intervening wires are not part of [the defendant's] house [or] office any more than are the highways along which they are stretched."[94] Looking inside a house from across the street with one's eyes through binoculars or using one's ears to listen to conversations inside a house was not classified as a physical trespass onto a person's home, a constitutionally protected area.

Furthermore, the Court viewed conversations as intangible and not constitutionally protected.[95] Finding that speech was not classified property within the Fourth Amendment's context, the Court determined that wiretapping did not constitute a search or seizure to trigger the Fourth Amendment's protection.[96] The Court's decision demonstrated that the Fourth Amendment's application depended on whether law enforcement trespassed on a suspect's constitutionally protected property. Since the Court decided that conversations and telephone line wires on a public street were not constitutionally protected property or areas under the Fourth Amendment, there was no constitutional violation.

B. 1961: Spike Mike

Silverman v. United States[97] concerned the applicability of the Fourth Amendment to warrantless use of a spike mike by government agents. A spike mike "was a microphone with a spike about a foot long attached to it together with an amplifier, a power pack, and

---

[90] *Id.* at 456-57.
[91] *Id.* at 466.
[92] *Id.* at 457.
[93] *Id.* at 466.
[94] *Id.* at 465.
[95] *Id.*
[96] *Id.* at 466.
[97] *See* Silverman v. United States, 365 U.S. 505 (1961).

earphones."[98] In this case, officers pushed a spike mike through a neighboring house until it touched the heating ducts occupied by the defendant's house.[99] The officers then heard the defendant's conversations from the second and first floors through the spike mike earphones.[100]

In determining whether law enforcement violated the defendant's Fourth Amendment right, the Court moved away from its decision in *Olmstead*[101] and decided that it was unnecessary to show an actual governmental trespass.[102] The Court did not need to examine whether there was a taking of physical property.[103] The Court stressed that "inherent Fourth Amendment rights are not inevitably measurable in terms of ancient niceties of tort or real property law."[104] The Court instead relied on the personal rights that the Fourth Amendment secures.[105] At 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."[106] The Court indicated it has "never held that a federal officer may without [a] warrant and without consent physically entrench into a man's office or home, there secretly observe or listen, and relate at the man's subsequent criminal trial what was seen and heard."[107] The Court held the actual intrusion into a constitutionally protected area, the defendant's home, was effected without the owner's knowledge or consent.[108] Consequently, there was no need to determine whether a technical trespass under property law occurred relating to the defendant's wall.[109] Accordingly, the Supreme Court was preparing to look beyond the property right, trespass analysis applied in *Olmstead*.[110]

---

98 *Id.* at 506.
99 *Id.* at 506-07.
100 *Id.*
101 *See* Olmstead, 277 U.S. 438 (1928).
102 *Silverman*, 365 U.S. at 510.
103 *Id.* at 511.
104 *Id.*
105 *Id.*
106 *Id.*
107 *Id.* at 512.
108 *Id.*
109 *Id.* at 511.
110 *See* Olmstead v. United States, 277 U.S. 438 (1928).

C. 1967: Electronic Listening and Recording Devices

In 1967, the Supreme Court decided a landmark decision regarding the Fourth Amendment and rejected the trespass on property analysis from *Olmstead*.[111] In *Katz v. United States*, the Court further elaborated on the protection of personal rights from *Silverman*[112] by establishing the "reasonable expectation of privacy"[113] doctrine. *Katz*[114] concerned the applicability of the Fourth Amendment to the government's warrantless use of an electronic listening and recording device attached to a public telephone booth.[115]

The Court asserted that the Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion."[116] More importantly, the "Fourth Amendment protects people[,] not places."[117] The Court considered the advancements of technology and decided that the trespass doctrine constituted "bad physics as well as bad law."[118] The Court determined that "what a person knowingly exposes to the public, even in his own home or office, is not subject to the Fourth Amendment['s] protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[119]

In this case, although people could see Katz in the glass fashioned telephone booth, they could not hear his conversations. The Court further stated, "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[120] The government agents ignored the Fourth Amendment's requirement of obtaining a search warrant based on probable cause. The Court reasoned that a warrant is "a constitutional precondition of the kind of electronic surveillance involved in this case."[121]

Justice Harlan's concurring opinion determined that the protection derived from the Fourth Amendment depends on a person's

---

111 *Id.*
112 *See Silverman*, 365 U.S. at 505.
113 *See* Katz v. United States, 389 U.S. 347 (1967).
114 *Id.*
115 *Id.* at 349-50.
116 *Id.*
117 *Id.* at 351.
118 *Id.* at 362 (Harlan, J., concurring).
119 *Id.* at 351. (internal citations omitted).
120 *Id.* at 359.
121 *Id.*

reasonable expectation of privacy.[122] Justice Harlan stated that a person's home is "a place where he expects privacy, but objects, activities or statements that he exposes to the plain view of outsiders are not protected because no intention to keep them to himself has been exhibited."[123] Similarly, "conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable."[124]

In this case, Justice Harlan reasoned that when Katz shut the door of the booth and paid to make his phone call, he was entitled to assume that his conversations were private.[125] Justice Harlan viewed the telephone booth as "a temporarily private place whose momentary occupants' expectations of freedom from [government] intrusion[s] are recognized as reasonable."[126] Thus, surveillance of a person's conversations in a public telephone booth was unreasonable, absent a search warrant.

D. 2001: Thermal Imaging Device

Kyllo v. United States[127] concerned the applicability of the Fourth Amendment to the government's warrantless use of a sense-enhancing device aimed at a private home from a public street. [128] In this case, agents suspected Kyllo of growing marijuana in his home, which required high-intensity lamps.[129] Agents used an Agema Thermovision 210[130] thermal imager device to scan Kyllo's home to detect infrared radiation that was invisible to the naked eye.[131] The thermal imager device operated like a "video camera showing heat images."[132] Kyllo's home scan took only a few minutes, and the agent

---

122 *Id.* at 361 (Harlan, J., concurring).

123 *Id.* (Harlan, J., concurring) (internal quotation marks omitted).

124 *Id.* (Harlan, J., concurring).

125 *Id.* (Harlan, J., concurring).

126 *Id.* (Harlan, J., concurring).

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

128 *Id.* at 29.

129 *Id.*

130 *Id.* (describing the Agema Thermovision 210 as a thermal imager, which detects infrared radiation which generally all objects emit but is not visible to the naked eye. The thermal imager converts the infrared radiation into images based on relative warmth. Black signifies that the area is cool, white shows the area is hot. Shades of gray suggest relative temperature differences. The thermal imager operates like a video camera showing heat images.).

131 *Id.*

132 *Id.* at 30.

obtained this data sitting across the street from the front of Kyllo's house.[133] The scan showed that the roof over the garage and a sidewall of Kyllo's home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes.[134]

The Court stated, "[a]t the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[135] The Court understood the concern over technological advancements and its impact on privacy rights by saying, "the rule we adopt must take account of more sophisticated systems that are already in use or in development."[136] The Court stated, "all details [from houses] are intimate details, because the entire area is held safe from prying government eyes."[137] The agent obtained details of how warm Kyllo heated his home, and the details were intimate because it was data collected from the home.[138] The Court stated, "[w]hile it is certainly possible to conclude from the videotape of the thermal imaging [device] that…no significant compromise of the homeowner's privacy [occurred], we must take the long view, from the original meaning of the Fourth Amendment forward."[139] Thus, the government's surveillance by a thermal-image device, which collected details of the home that were not visible without entering the home, was a search and was unreasonable without a warrant.[140]

E. 2012: GPS

United States v. Jones[141] concerned the applicability of the Fourth Amendment to the government's use of a GPS tracking device without a valid warrant.[142] In *Jones*, government officials acquired a warrant to expire in ten days that authorized installing a GPS device on the car registered to Jone's wife in the District of Columbia.[143] On

---

133 *Id.*
134 *Id.*
135 *Id.* at 31 (internal quotation marks omitted.)
136 *Id.* at 36.
137 *Id.* at 37.
138 *Id.* at 38.
139 *Id.* at 40.
140 *Id.*
141 *See* United States v. Jones, 565 U.S. 400 (2012).
142 *Id.*
143 *Id.* at 402-03.

the eleventh day, government officials installed the GPS tracking device on the car's undercarriage in Maryland without a valid, legally binding warrant.[144] Over the next twenty-eight days, government officials used the device to track the car's movements.[145] Officials also replaced the GPS's battery located on the car.[146]

The Court recognized that "[b]y means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer. It relayed more than 2,000 pages of data over the 4-week period."[147] The Court stated, "[i]t is beyond dispute that a vehicle is an "effect" as that term is used in the Amendment."[148] Here, law enforcement physically occupied private property and obtained incriminating information.[149] Thus, the government's installation of the GPS device on the car to monitor its movements constituted a search under the Fourth Amendment.[150]

In reaching its decision, the Court considered the framers' intent in drafting the Constitution. The Court stated, "[t]he text of the Fourth Amendment reflects its close connection to property, since otherwise[,] it would have referred simply to the right of the people to be secure against unreasonable searches and seizures."[151] The Court reasoned that Jones possessed the car, "at the time the Government trespassorily inserted the information gathering [GPS] device."[152] Here, the Court focused on the prior property-based trespassory analysis of the Fourth Amendment. However, the Court did state, "we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would remain subject to the [reasonable expectation of privacy] analysis."[153]

Justice Sotomayor's concurring opinion emphasized that the Fourth Amendment did not only apply to government trespassory intrusions on private property.[154] The reasonable expectation of

---

144 *Id.* at 403.
145 *Id.*
146 *Id.*
147 *Id.*
148 *Id.* at 404.
149 *Id.*
150 *Id.*
151 *Id.* at 405 (internal quotation marks omitted).
152 *Id.* at 410.
153 *Id.* at 411.
154 *Id.* at 414 (Sotomayor, J., concurring).

privacy analysis "augmented, but did not displace or diminish, the common-law trespassory test that preceded it."[155] Justice Sotomayor stated, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[156] Considering that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations[,]"[157] it is clear that officers need warrants to obtain this data. Furthermore, GPS monitoring is "cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices."[158]

More importantly, Justice Sotomayor thought it might "be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[159] Justice Sotomayor believed the third party doctrine was "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[160] Justice Sotomayor determined that consumers of electronic devices "can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy."[161] She further stated, "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[162] Justice Sotomayor acknowledged the growing concern that people who use electronic devices might be left unprotected under the law.

F. 2014: Cell Phone

Riley v. California[163] concerned the applicability of the Fourth Amendment to the government's search of cell phones without a warrant. In *Riley*, an officer confiscated Riley's "smart phone, a cell

---

155 *Id.* (Sotomayor, J., concurring).
156 *Id.* at 415 (Sotomayor, J., concurring).
157 *Id.* (Sotomayor, J., concurring).
158 *Id.* at 415-16 (Sotomayor, J., concurring).
159 *Id.* at 417 (Sotomayor, J., concurring).
160 *Id.* (Sotomayor, J., concurring).
161 *Id.* at 418 (Sotomayor, J., concurring).
162 *Id.* (Sotomayor, J., concurring).
163 *See* Riley v. California, 573 U.S. 373 (2014).

phone with a broad range of other functions based on advanced computing capability, large storage capacity[,] and Internet connectivity."[164] Without a warrant, the officer searched the cell phone.[165]

Here, the Court considered that "cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."[166] Cell phones are "minicomputers that also happen to have the capacity to be used as a telephone."[167] The Court acknowledged that a distinguishable feature of modern cell phones is their immense storage capacity.[168] Before cell phones, a search of a person resulted in gathering limited information that "constituted only a narrow intrusion on privacy."[169] However, technology advanced to the degree where law enforcement can obtain detailed information about the owner of the cell phone:

> Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read–nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant…rather than a container the size of the cigarette package.[170]

Therefore, the investigations of cell phones reveal more detailed information about an arrestee then ever before.

The Court determined that law enforcement's intrusion into privacy is no longer physically limited due to cell phones. For example, cell phone technology translates millions of "pages of text, thousands of pictures, or hundreds of videos."[171] Also, "even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on."[172] The Court noted, it is no

---

164 *Id.* at 379.
165 *Id.*
166 *Id.* at 393.
167 *Id.*
168 *Id.*
169 *Id.*
170 *Id.* at 393-94.
171 *Id.* at 394.
172 *Id.*

exaggeration to say that about "90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives–from the mundane to the intimate."[173]

Obtaining cell phone data differs from physical evidence not only in quantity but also in quality. "An Internet search and browsing history, for example, can be found on an Internet-enabled phone and [can] reveal an individual's private interest or concerns–perhaps a search for certain symptoms of [a] disease, coupled with frequent visits to WebMD [will show a user's worry over an illness.]"[174] The Court also considered users' ability to download other applications onto their phones:

> Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase "there's an app for that" is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life.[175]

A single cell phone could give officials access to information that would generally require long hours of surveillance and, even then, would not result in readily available information as a cell phone.

Moreover, the data users view on their cell phones may not be stored on the device:

> [C]ell phones [are] used to access data located elsewhere, at the tap of a screen. That is what cell

---

[173] *Id.* at 395.
[174] *Id.* at 395-96.
[175] *Id.* at 396.

> phones, with increasing frequency, are designed to do by taking advantage of 'cloud computing.' Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference. Moreover, the same type of data may be stored locally on the device for one user and in the cloud for another.[176]

A cell phone could equip officers with information recorded at the time of the arrest, and information that was recorded several months or years ago because of cloud storage.

The Court determined it was reasonable to expect that "incriminating information will be found on a phone regardless of when the crime occurred."[177] The Court stated that "even an individual pulled over for something as basic as speeding might well have locational data dispositive of guilt on his phone."[178] Likewise, "an individual pulled over for reckless driving might have evidence on the phone that shows whether he was texting while driving."[179]

The Court stated, "modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life."[180] The Court held, "the fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."[181] Thus, the Court concluded that cell phones are distinct from other physical material, resulting in a warrant requirement.[182] The Court's holding "is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search."[183]

---

176 *Id.* at 397 (internal citation omitted).
177 *Id.* at 399.
178 *Id.*
179 *Id.*
180 *Id.* at 403 (internal quotation marks and citation omitted).
181 *Id.*
182 *Id.* at 381.
183 *Id.* at 401.

G. 2018: Cell Site Location

Carpenter v. United States[184] concerned the applicability of the Fourth Amendment to the government's seizure and search of cell site location information from cell phone companies.[185] In *Carpenter*, officers obtained "12,898 location points cataloging Carpenter's movements–an average of 101 data points per day"[186] from cell phone companies. Cell site location information (CSLI) is the time-stamped record that a phone produces when it connects to a cell site,[187] radio antennas.[188] The Court noted that "most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even [when] the owner is not using one of the phone's features."[189]

In determining whether the Fourth Amendment applied, the Court reviewed past cases dealing with technological advancements. The Court stated, "the Amendment seeks to secure the privacies of life against arbitrary power."[190] Also, a "central aim of the Framers was to place obstacles in the way of a too permeating police surveillance."[191] However, this case was different from previously decided cases as third party cell phone companies maintained the CSLI, which did not fit neatly under existing precedent.[192]

The Court analyzed whether the third party doctrine applied to CSLI, which would allow law enforcement to obtain CSLI without a warrant. In past cases, the Court distinguished the application for the Fourth Amendment between information that people kept private and information shared with others. The third party doctrine determines that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[193] The law applies, "even if the information is revealed on the assumption that it will be used only for a limited purpose."[194]

---

184 *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).
185 *Id.*
186 *Id.* at 2212.
187 *Id.* at 2211.
188 *Id.*
189 *Id.*
190 *Id.* at 2214 (internal quotation marks omitted).
191 *Id.*
192 *Id.*
193 *Id.* at 2216 (quoting Smith v. Maryland, 442 U.S. 735, 743 (1979)).
194 *Id.* (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).

The third party doctrine originated from *United States v. Miller*,[195] where Miller could "assert neither ownership nor possession"[196] of his bank statements since the Court determined the documents were part of the bank's business records. In *Miller*, the checks and bank statements were "not confidential communications but negotiable instruments to be used in commercial transactions."[197] This further showed that Miller had a limited expectation of privacy in those documents. Furthermore, Miller exposed the bank statement's information to bank employees in the "ordinary course of business."[198] Thus, the Fourth Amendment did not protect Miller's bank statements.[199]

Additionally, the Court applied the third party doctrine in the context of information conveyed to a telephone company.[200] In *Smith v. Maryland*,[201] the Court ruled that government officials' use of a pen register, a device that recorded the outgoing phone numbers dialed on a landline telephone, was not a search.[202] Since a pen register had limited capabilities in its use, the Court "doubt[ed] that people[,] in general[,] entertain any actual expectation of privacy in the numbers they dial."[203] Also, telephone subscribers knew that telephone companies used numbers dialed for a variety of legitimate business purposes, including routing calls.[204] Thus, when Smith placed a call, he "voluntarily conveyed the dialed numbers to the phone company by exposing that information to its equipment in the ordinary course of business."[205] Thus, the Fourth Amendment did not protect the numbers Smith dialed.[206]

However, in Carpenter's case, the Court faced a new phenomenon that did not fit with past decisions: the ability to chronicle a person's past movements through the record of his cell phone signals.

---

195 *See Miller*, 425 U.S. at 435.
196 *See Carpenter*, 138 S. Ct. at 2216 (quoting *Miller*, 425 U.S. at 440).
197 *Id.* (quoting *Miller*, 425 U.S. at 440).
198 *Id.* (quoting *Miller*, 425 U.S. at 442).
199 *Id.* (quoting *Miller*, 425 U.S. at 443).
200 *See* Smith v. Maryland, 442 U.S. 735 (1979).
201 *Id.*
202 *Carpenter*, 138 S. Ct. at 2216 (quoting *Smith*, 442 U.S. at 742).
203 *Id.* (quoting *Smith*, 442 U.S. at 742).
204 *Id.* (quoting *Smith*, 442 U.S. at 743) (internal quotation marks omitted).
205 *Id.* (quoting *Smith*, 442 U.S. at 744) (internal quotation marks omitted).
206 *Id.* (quoting *Smith*, 442 U.S. at 745).

CSLI is "detailed, encyclopedic, and effortlessly compiled."[207] Since users share this information with their telephone companies, the third party doctrine applies. However, the Court expressly declined to apply the third party doctrine to cover this new circumstance.[208]

Given the unique nature of cell phone location records, the fact that a third party holds this information does not overcome the user's claim to Fourth Amendment protection.[209] The Court reasoned that "although [CSLI] records are generated for commercial purposes, that distinction does not negate Carpenter's anticipation of privacy in his physical location."[210] The Court stated, "mapping a cell phone's location [for] 127 days provides an all-encompassing record of the holder's whereabouts."[211]

In distinguishing GPS tracking with CSLI, the Court stated, "a cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[212] More importantly, the Court noted that wireless carriers maintain phone records for up to five years.[213] The continuously logged CSLI affects all cell phone users, not just people under investigation.[214]

The Court determined that the current third party doctrine did not apply to CSLI. The Court stated, "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."[215] For example, phone companies are not typical witnesses, unlike a "nosy neighbor."[216] Hence, granting law enforcement access to CSLI without a warrant would grant a "significant extension of [the third party doctrine] to a distinct category of information."[217]

Likewise, users did not voluntarily share their CSLI with their wireless providers. The Court stated, "a cell phone logs a cell-site

---

207 *Id.*
208 *Id.* at 2217.
209 *Id.*
210 *Id.*
211 *Id.*
212 *Id.* at 2218.
213 *Id.*
214 *Id.*
215 *Id.* at 2219.
216 *Id.*
217 *Id.*

record by dint of its operation, without an affirmative act on the part of the user beyond powering up."[218] The CSLI was generated by virtually any activity conducted on the phone. The Court noted that "apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[219] The Court determined that "in no meaningful sense does the user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements."[220]

The Court held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[221] Thus, where a suspect has a legitimate privacy interest in records held by a third party, like CSLI, the government needs a warrant.[222] However, in this case, the Court did not decide on the issue of "real-time CSLI or 'tower dumps' (a download of information on all the devices connected to a particular cell site during a particular interval)."[223]

IV. WAYS TO MOVE FORWARD: ALEXA-ENABLED SMART HOME DEVICES PROTECTED UNDER CURRENT FEDERAL LAW

A. The Reasonable Expectation of Privacy Doctrine Applied to Alexa-Enabled Smart Home Devices

According to *Katz*,[224] the Fourth Amendment applies when a person has a reasonable expectation of privacy in the place or item searched or seized.[225] Arguably, people hold a reasonable expectation of privacy in their Alexa-enabled smart home devices because of the quality and quantity of information the device records and stores. Not only does the Alexa-enabled smart home device function as a telephone, but it also functions as a virtual assistant controlling other smart home devices and keeping the user organized.

However, the Court previously determined that "what a person knowingly exposes to the public, even in his own home or office, is

---

218 *Id.* at 2220.
219 *Id.*
220 *Id.* (internal quotation marks omitted).
221 *Id.* at 2217.
222 *Id.*
223 *Id.* at 2220.
224 *See* Katz v. United States, 389 U.S. 347 (1967).
225 *Id.* at 351.

not subject to the Fourth Amendment protection."[226] Similarly, "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[227] Users of Alexa-enabled smart home devices run the risk that Alexa is accidentally recording their conversation since Alexa is continuously listening for its wake word. What a user seeks to preserve as private might involuntarily be exposed to the public. For example, if, in the privacy of their bedroom, a couple starts to argue and Alexa starts recording without the couple's knowledge, then arguably, the couple has a reasonable expectation of privacy in the communications recorded by Alexa.

The government might argue that users of smart home devices do not have a reasonable expectation of privacy in the device or its recordings because they share the information with Amazon. However, the couple did not knowingly expose their argument to the public since they did not call on Alexa for assistance. Moreover, the couple chose to argue in the privacy of their bedroom where no one can see or hear them. The couple can claim that they had a reasonable expectation of privacy in their Alexa-enabled smart home device and its recordings because it accidentally recorded information about the owners.

The couple would also be entitled to claim that they never intended their intimate conversations to be accessed so easily by the government. The Supreme Court has always held that a person's home is a place where he expects privacy.[228] When the couple shut the front door of their home, they held a reasonable expectation of privacy and expected to be free from unlawful government intrusion.

The Supreme Court has already found that collecting intimate details from within a home is a search and unreasonable.[229] The data collected from Alexa-enabled smart home devices reveal specific details of the home where one holds a reasonable expectation of privacy. For example, when a user sets a routine on Alexa to drop the heating temperature and gradually turn on the lights, Alexa is recording the requests. This information not only shows the electricity usage and heating consumption in the home but also reveals the home owner's preferences.

---

226 *Id.*

227 *Id.*

228 *Id.* at 361.

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

Government officials' access to Alexa's recorded transcripts would disclose information that would be impossible to see without entering the user's home. As in *Kyllo*,[230] the law holds that law enforcement's obtaining such intimate details of a home is a search that requires a warrant.[231] Since the Court held that detailed information collected about actions from within a home requires a warrant,[232] the government should also obtain a warrant to search or seize Alexa-enabled smart home devices. Amazon created Alexa-enabled smart home devices for home use, and these devices record information about the user in his home. The home is a constitutionally protected area where people have a reasonable expectation of privacy. Thus, people have a reasonable expectation of privacy in their Alexa-enabled smart home devices and their recordings.

B. The Property-Based Trespassory Analysis Applied to Alexa-Enabled Smart Home Devices

The Fourth Amendment can also protect Alexa-enabled smart home devices through the property based trespassory analysis of the Fourth Amendment. The Court previously held that a physical trespass by law enforcement constitutes an unreasonable search and seizure.[233] As to the car in *Jones*,[234] a user's Alexa-enabled smart home device is personal property that should also fall under the category of effects listed in the amendment.[235] For example, if law enforcement were to grab a home owner's Alexa-enabled smart home device, this would constitute a trespass onto the user's personal property. A search warrant is required by law enforcement to search and seize a user's Alexa enabled smart device as in *Jones*,[236] where law enforcement physically occupied private property and obtained incriminating information.[237]

Moreover, the Court explicitly left the door open for Alexa-enabled smart devices, whose data transmission does not necessarily require physical trespass, for the reasonable expectation of privacy

---

230 *Id.* at at 27.
231 *Id.* at 40.
232 *Id.* at 38.
233 United States v. Jones, 565 U.S. 400, 410 (2012).
234 *Id.*
235 *Id.* at 404.
236 *Id.*
237 *Id.*

analysis.[238] Like GPS devices, Alexa-enabled smart home devices can reveal a user's daily route to work by reviewing the transcript, which would show how many times the user asked Alexa to check the fastest way to travel to work.

Like GPS devices, Alexa can record the user's movements, but in a different context. Instead of showing a user's location through signals from multiple satellites, Alexa's recording history can show the user's past movements through the aggregate collection and analysis of Alexa's recording transcripts. For example, the transcript created by Alexa's continuous recording would show that the user frequently visited the doctor's office by reading the transcript where the user asked Alexa to schedule weekly appointments in the online calendar. Nevertheless, law enforcement's search of the user's personal property, the Alexa-enabled smart home device, is a physical trespass under the Fourth Amendment that requires a search warrant.

C. Alexa-Enabled Smart Home Devices Should be Treated as Cell Phones

Under *Riley*,[239] the Fourth Amendment applies to the search and seizure of a smartphone with similar abilities to Alexa-enabled smart home devices.[240] In *Riley*, the Court held that law enforcement's intrusion of privacy is no longer physically limited due to cell phones.[241] Before smartphones and Alexa-enabled smart devices, law enforcement could only obtain limited data about an individual, let alone information from within his home. Like the smartphone in *Riley*, Alexa-enabled smart home devices have massive storage capacity.

Today, when officers obtain Alexa-enabled smart home devices, they see all the tasks and questions posed by the user to Alexa. As with smartphones, officers can obtain detailed information about users from their smart home devices. For example, the recordings by Alexa produce transcripts that enable law enforcement to see or hear the conversations made during the time that a crime ensued. If the user asks Alexa to search for the nearest firearms and gun store on the day before committing murder, that information might show that he had the prerequisite intent to cause the death of another person. This

---

238 *Id.* at 411.

239 *See* Riley v. California, 573 U.S. 373 (2014).

240 *Id.* at 401.

241 *Id.* at 394.

scenario is similar to how a cell phone might show law enforcement that the user was driving recklessly because, at the time of the accident, his cell phone shows he was streaming a live video on social media. Depending on what law enforcement finds on a smart home device may lead to a criminal conviction.

Furthermore, like smartphones, the data from Alexa-enabled smart home devices differ from physical evidence in quantity and quality. Alexa connects users to the internet and other smart devices and records these actions. An internet search and browsing history can reveal the user's private interest or concerns. Alexa-enabled smart home devices hold many people's private information about their lives, just like smartphones. As the Court stated, "the fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."[242] Even though people do not usually carry around the Alexa-enabled Echo device, it still stores and collects a large scale of personal information that warrants protection under the Fourth Amendment.

D. The Third Party Doctrine and Alexa-Enabled Smart Home Devices

The third party doctrine should not apply to prohibit people from claiming Fourth Amendment protection over their smart home devices. The third party doctrine states that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[243] The law applies "even if the information is revealed on the assumption that it will be used only for a limited purpose."[244] Whenever a user makes a voice request, the Alexa-enabled smart home device records the user's speech and stores the data on Amazon's servers, or cloud system, thus possibly implicating the third party doctrine. However, as in *Carpenter*,[245] where the third party doctrine did not apply to the government's seizure and search of CSLI from wireless carriers, the Court should rule similarly with Alexa-enabled smart home devices

---

[242] *Id.* at 403.

[243] Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (quoting Smith v. Maryland, 442 U.S. 735, 743 (1979)).

[244] *Id.* (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).

[245] *Id.* at 2206.

In order to function at its highest capacity, Alexa-enabled smart home devices need to connect wirelessly to other data networks and the cloud system. Amazon's Alexa-enabled Echo device activates with the wake word "Alexa"[246] and immediately connects to servers or other smart devices to fulfill the user's request. The user's voice is recognized by Alexa,[247] which allows the device to access content on the internet, specifically for the user. The data recorded is stored unless the user deletes it. To illustrate, users of Amazon's Echo device can manage and delete their audio recording transcripts through the Alexa App or by asking Alexa to delete the recordings.[248]

Alexa-enabled smart home devices should overcome the implementation of the third party doctrine and the doctrine's result because sharing information with a third party does not by itself bar it from Fourth Amendment protections. As CSLI in Carpenter, the data collected and recorded by Alexa is detailed and automatically compiled. Like CSLI, Alexa-enabled smart home devices share information with a third party, Amazon's employees, to improve the device and delivery system. The Court in *Carpenter* stated, "although [CSLI] records are generated for commercial purposes, that distinction does not negate Carpenter's anticipation of privacy in his physical location."[249] A stack of Alexa's recorded transcripts can reveal a user's past physical movements and potential future appointments.

Arguably, the third party doctrine should not apply towards data collected from Alexa-enabled smart devices. Since Alexa can tell users the traffic conditions and inform users about the duration of their commute,[250] a print-out of these requests would show the user's location at a specific time. For example, a month's worth of transcripts containing the interactions between the user and Alexa reveals a detailed record of the user's whereabouts. CSLI can reveal when a person visited the doctor's office. However, Alexa-enabled smart home devices can show the same information through recordings and transcripts and detail the purpose of the visit.

---

246 Weiss, *supra* note 2.

247 *Alexa Features: News & Information*, *supra* note 71.

248 Katie Conner, *Here are the Best Tips for Keeping your Information Private While Using Alexa*, CNET https://www.cnet.com/how-to/have-amazon-echo-privacy-fears-heres-what-you-can-do/ (Oct. 24, 2019).

249 *Carpenter*, 138 S. Ct. at 2217.

250 *Alexa Features: News & Information*, *supra* note 71.

More importantly, like CSLI, Alexa's constant listening ability affects all users, not just those under an investigation. As CSLI collects unlimited personal information about the user's physical movements, Alexa-enabled devices collect significantly more detailed information. Arguably, just as the wireless carriers in Carpenter were not typical witnesses, Amazon itself should not be considered a typical witness.

On the other hand, the government could argue that the third party doctrine should apply to data collected from Alexa-enabled smart devices because people voluntarily share their recorded information with Amazon. Alexa-enabled devices upload the recordings to Amazon's servers, and they are used to conduct improvements on the devices. Similarly, cell phones log CSLI, which are collected and maintained by wireless providers. Regarding CSLI, the sharing of cell phone data with wireless providers is not enough to bar the Fourth Amendment's protection.

A person's mere usage creates CSLI without taking any affirmative action to authorize such data collection except for powering up the device.[251] Similarly, Alexa records a person's conversations without the need for users to hit a record button physically. Like cell phones, apart from shutting off the Alexa-enabled device, there is no way to avoid Alexa's recording of the user's speech.

The Court determined in *Carpenter* that "in no meaningful sense does the user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements."[252] Contrary to what the government might argue, users of Alexa-enabled smart home devices do not voluntarily disclose the complete documentation of all encounters and conversations in their homes through the use of Alexa. Arguably, a warrant should be required when users have a legitimate privacy interest in records held by a third party like Amazon.

V. REDEFINING THE TERM "EFFECTS" TO INCLUDE ALEXA-ENABLED SMART HOME DEVICES

The Fourth Amendment of the United States Constitution reads:

---

[251] *Carpenter*, 138 S. Ct. at 2220.

[252] *Id.* (internal quotation marks omitted).

> [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 Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularity describing the place to be searched, and the persons or things to be seized.[253]

This Note began by acknowledging that the framers of the United States Constitution did not have a reason to develop law concerning the government's use of smart technology to acquire, store, and analyze personal information about Americans.[254] When the founding fathers drafted and ratified the Constitution, there were no electronic devices such as satellites, cell sites, GPS, cell phones, or other smart devices. For these reasons, Andrew Guthrie Ferguson[255] explored how the "Fourth Amendment built on old-fashioned 'effects' can address a new world in which things are no longer just inactive, static objects, but objects that create and communicate data with other things."[256] Ferguson concluded that "unless our constitutional understanding of an effect adapts to meet modern technology, smart objects will be open to warrantless searches without sufficient Fourth Amendment protection."[257]

Ferguson argued that the term effects under the Fourth Amendment should include smart objects and the related data that the object transmits into the "Internet of Things."[258] Thus, effects should encompass the smart device's "functionality[,] including its necessary communication with other devices and stored data."[259] Thus, according to Ferguson, an effect would consist of the physical object, smart data, and communicating signals emanating from the device.[260]

---

[253] U.S. CONST. amend. IV.

[254] Jones, *supra* note 5.

[255] Professor of Law, David A. Clarke School of Law at the University of the District of Columbia.

[256] Ferguson, *supra* note 11, at 808.

[257] *Id.*

[258] *Id.* at 813 (introducing Technologist Kevin Ashton as the person who coined the term 'the Internet of Things' in 1998. Kevin Ashton stated, "adding radio-frequency identification and sensors to everyday objects will create an Internet of Things, and lay the foundations of a new age of machine perception."). *Id.*

[259] *Id.* at 809.

[260] *Id.*

Under Ferguson's definition of effects, sensory-embedded license plates would be afforded constitutional protection from the term effects.[261] Ferguson classified things as effects if they were "(1) an identifiable object (2) that wirelessly communicates information about the object and (3) is linked to sensors that read information about the object."[262] Ferguson's new definition of effects would cover smart objects that relay data to collecting sensors.[263]

The term "'effects' in the Fourth Amendment has long been understood to signify the protection of personal property."[264] With this in mind, the Supreme Court has referenced particular objects as effects such as weapons and fruits of a crime,[265] clothing,[266] automobiles,[267] luggage,[268] and other containers. The modern-day approach to effects seen in *Jones* focused on the physical search of a car, an effect.[269] Similarly, in *Riley*, law enforcement searched the digital information stored on a smartphone, an effect.[270] Ferguson determined that in *Riley*, the Court's "distinction between physical objects and [smart] objects [broke] new ground for the Supreme Court, opening the door to perhaps a different analysis for digital information."[271]

According to Ferguson, "the appropriate analysis to determine whether the communication of [a smart device] can be intercepted and seized is whether the sensor data and signals fall within the constitutional interest of a smart effect."[272] Since the data and signals are at the core of smart devices, Ferguson argued that both should be considered part of the redefined Fourth Amendment term effects.[273]

Sensor data and signals fall within the constitutional property interest of a smart device. The Fourth Amendment protects both tangible[274] and intangible property.[275] Underlying these protections

---

261 *Id.* at 824.
262 *Id.*
263 *Id.*
264 *Id.*
265 *See* Warden v. Hayden, 387 U.S. 294 (1967).
266 *See* United States v. Edwards, 415 U.S. 800 (1974).
267 *See* United States v. Chadwick, 433 U.S. 1 (1977).
268 *See* Bond v. United States, 529 U.S. 334 (2000).
269 United States v. Jones, 565 U.S. 400, 404 (2012).
270 Riley v. California, 573 U.S. 373, 381 (2014).
271 Ferguson, *supra* note 11, at 834.
272 *Id.* at 859.
273 *Id.*
274 *See Jones*, 565 U.S. at 404.
275 *See* Katz v. United States, 389 U.S. 347 (1967).

over tangible and intangible property is that property is of value to the user.[276] As Ferguson states, "the data is a valuable part of the ownership interest in the effect."[277] The information collected from smart devices is "largely private, encompassing sensitive home, personal travel, and health information[,] among other things."[278]

Alexa-enabled smart home devices would fall under Ferguson's new definition of effects because the smart home device is a thing, which emanates data to Amazon's servers and connects users to the internet and other smart devices. Alexa-enabled smart home devices, classified under Ferguson's definition of effects, would afford it constitutional protection both in the device and in its contents. The constitutional property interest that users of smart devices hold is not just in the physical device but in the data transmitted to Amazon servers.

An argument against extending the term effects to the data that the smart device emanates is the view that the user does not exclusively own the data because the user must share the data with a third party. In response, the Court has already determined, in regard to CSLI, that law enforcement needs a warrant to obtain records held by a third party where a person has a reasonable expectation of privacy in the information.[279] Since the Court determined that law enforcement's acquisition of data collected from ceaseless monitoring devices requires a warrant, Alexa-enabled smart home devices will similarly require a warrant since the transcripts from Alexa's recordings will reveal a user's past location history.

Moreover, Ferguson purported that for Fourth Amendment purposes, "coownership does not remove the ability to exclude"[280] data collected by smart home devices from government interference. Smart home device owners have "a claim to control the data and a right to exert a measure of control excluding the government from any attempt at direct collection."[281] Thus, it appears that smart devices, as effects, should be considered among other recognized constitutionally protected property.[282]

---

[276] Ferguson, *supra* note 11, at 860.

[277] *Id.*

[278] *Id.* at 863.

[279] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[280] Ferguson, *supra* note 11, at 861.

[281] *Id.*

[282] *Id.* at 832. *See* Oliver v. United States, 466 U.S. 170,177 (1984).

VI. DIGITAL CURTILAGE FRAMEWORK

Ferguson proposed the theory of digital curtilage as a framework to address the advancement of technology and the concern over privacy rights.[283] Although no court has used this framework, it is relevant to show that this new theory would protect smart home devices and their data if adopted by courts. This Note discusses Ferguson's digital curtilage framework and analyzes how it would protect Alexa-enabled smart home devices and their data from unreasonable searches and seizures.

The principles of traditional curtilage inspired Ferguson's digital curtilage framework.[284] Ferguson's digital curtilage theory aimed to protect "stored data and certain communication signals [that]: (1) are closely associated with the effect; (2) have been marked out and claimed as secure from others; and (3) are used to promote personal autonomy, family, self-expression, and association."[285] Ferguson holds that these factors can apply to his expanded definition of the term effects in the Fourth Amendment.[286] For the application of digital curtilage towards a smart device, the "smart effect [must] include: (1) data and signals that are closely associated with the effect; (2) data and signals that have been marked out and claimed as secure from others; and (3) data and signals used to promote personal autonomy, family, self-expression, and association."[287] Ferguson's digital curtilage, like traditional curtilage, provides a fact-based and balanced constitutional framework.[288]

First, digital curtilage will apply towards a smart device that includes data and signals closely associated with the effect.[289] Data stored on smart effects, like Alexa-enabled smart home devices, are closely associated with the device. The user needs to connect to the device itself to retrieve the data from Alexa-enabled smart home devices. This demonstrates the close connection between the data collected and the object that stores the information. Since the data

283 *Id.* at 809.
284 *Id.*
285 *Id.*
286 *Id.* at 866-67.
287 *Id.* at 867.
288 *Id.*
289 *Id.*

derives from a constitutionally protected device, under Ferguson's new effects definition, it benefits from the derivative protection.

Also relevant in the digital era is the term close, which does not mean a physical closeness because "the fluidity of data travel, duplicate, and overcome physical barriers."[290] Ferguson stated, "because smart data is part of the thing itself, and because the thing was designed to communicate smart data, then the data should be considered closely associated with the effect itself."[291]

Moreover, the data storage and the use of the smart device becomes a property right which a user can control. Ferguson believed that "at a minimum, consumers should be able to exclude others from the digital property."[292] Ferguson's theory would cover Alexa-enabled devices since users can manage and delete their audio recording transcripts through the Alexa App or by asking Alexa to delete their recordings.[293]

Users can make a strong claim that the data collected from the Alexa-enabled device is associated with the device. The Alexa-enabled smart home device's purpose is to help homeowners organize their lives by connecting to the internet and other smart home appliances and applications. Alexa-enabled smart home devices and the data they emanate satisfy Ferguson's first factor to apply digital curtilage. Ferguson stated, "because the information comes from a smart device, the data will be considered a part of this smart device…in the same way the curtilage principle extends protection of the home outside the home, so digital curtilage extends protection of data outside the smart effect."[294]

Second, digital curtilage will apply towards a smart device that includes data and signals that the user marked out and claimed as secure from others.[295] This part of the test will "narrow the scope of the protection for certain smart devices."[296] A user's exclusion under these circumstances is evident in the steps taken to secure the smart device data from others. For example, users can "secure a Wi-Fi

---

290 *Id.*

291 *Id.*

292 *Id.* at 868.

293 Conner, *supra* note 248.

294 Ferguson, *supra* note 11, at 868.

295 *Id.*

296 *Id.*

system through encryption."[297] Likewise, smartphones allow users to "opt out of locational tracking and other sharing requests."[298]

The "'marked and claimed as secure' factor requires an examination of how the creator of the data interacts with others seeking to collect data."[299] Ferguson assumed that since stored data lives within the effect, a presumption of security exists.[300] He further stated that "while stored data might remain unencrypted or even unprotected, because of its location in an effect, it retains constitutional protection."[301] This assumption extends existing law that protects stored data in smartphones.[302] Thus, under this step, courts will need to examine what actions users took to mark and secure the data from others.[303]

Alexa-enabled smart home devices and the data they transmit satisfy Ferguson's second factor to apply digital curtilage. Users of Alexa-enabled smart home devices can raise a virtual wall to keep other people from accessing their stored information. The data that Alexa records is stored unless the user deletes it. A user's affirmative act of deleting his Alexa audio recording transcripts by asking Alexa to delete his recordings will signal a desire to secure the information. When a user changes the wake word that triggers Alexa to respond and record, that is evidence that a user took an affirmative act to secure the device's use and access.

Ferguson further stated, "even if sophisticated hackers could thwart these types of security measures, a symbolic statement of security exists. After all, just because burglars and police can enter locked houses, it does not mean citizens lose a claim of security behind those walls."[304] Alexa-enabled smart home devices carry the option to secure the data and communications recorded by Alexa. Thus, when the user takes affirmative steps to claim security in the device, this factor is satisfied.

Third, digital curtilage will apply towards a smart device that includes data and signals used to promote personal autonomy, family,

---

297 *Id.*
298 *Id.*
299 *Id.* at 869.
300 *Id.*
301 *Id.*
302 *Id.*
303 *Id.*
304 *Id.*

self-expression, and association.[305] Ferguson determined that this step will further refine or limit the protections afforded to these effects.[306] More importantly, "a focus on data and signals from objects linked to personal or private matters will limit the expanded definition [of Ferguson's definition] of effects."[307]

Ferguson recognized that "[p]rotecting only personal and family-use data is consistent with the intent of traditional, physical curtilage."[308] Traditional curtilage protects areas that encourage home-like activities.[309] Similarly, in the digital context, "this understanding would protect expressive, associational, religious, family, personal, and dignity interests as opposed to unrevealing or impersonal data."[310] Ferguson's digital curtilage theory is subject to the same principles applied in traditional curtilage:

> As a result, the Fourth Amendment has been read to encourage an expansive vision of human development free from governmental surveillance. Thus, the personal and family interest argument should not be seen as a content-based test, but merely a recognition that many of the things we do (with or without smart objects) are done for personal growth and development. While at first blush this distinction might seem arbitrary, it is the same type of distinction that separates a protected curtilage space from an unprotected open field. Constitutionally protected interests are not just determined by property concepts (where you are standing) but also by privacy values and concerns about human autonomy that inform these conceptions of property (what you could be doing in that space).[311]

Protecting only personal and family use data will further refine and limit the protections afforded to these smart effects.

Alexa-enabled smart home devices promote personal autonomy, family, self-expression, and association. Alexa recognizes

---

[305] *Id.* at 870.
[306] *Id.*
[307] *Id.*
[308] *Id.*
[309] *Id.*
[310] *Id.* at 871.
[311] *Id.*

its user's voice, which allows the device to personalize the content shown.[312] The Alexa-enabled smart home device connects users to their personalized choice of entertainment. Alexa also personalizes a user's daily news updates.

Moreover, Alexa-enabled smart home devices allow users to communicate with anyone, anywhere, at any time.[313] Without touching any device, users can go through a day's worth of emails because Alexa can even read the user's emails out loud.[314] Furthermore, a significant development in Amazon's smart home device is its ability to handle and access a user's patient health information. Thus, by design Alexa promotes personal autonomy, family, self-expression, and association.

A strong argument against the theory of digital curtilage is the requirement that data and signals must be marked out and claimed as secure from others. Unlike traditional curtilage, where people must physically take steps to protect the alleged curtilage area from observation by passersby, digital curtilage does not require tremendous effort to keep the data secure. According to Ferguson's theory, a user of an Alexa-enabled smart home device would only need to change its wake word to constitute an affirmative act of securing the data.

The digital curtilage framework might be too lenient because it takes minimal action to show that the user protected the data from disclosure. This theory does not take into consideration that smart devices connect and share information with other networks. Many people download applications on their smart devices, which requires the dissemination of their information to make their device more efficient. The requirement to secure the data embedded in smart devices shared with other sensor devices leads to a potential technological theory of the third party doctrine. The third party doctrine holds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[315] Since smart devices share a user's information with other smart devices and other servers, the government can argue that the information is therefore not secured.

---

[312] *Alexa Features: News & Information*, *supra* note 71.

[313] *Alexa Features: Smart Home*, *supra* note 67.

[314] *Alexa Features: Productivity*, *supra* note 75.

[315] Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (quoting Smith v. Maryland, 442 U.S. 735, 743 (1979)).

VII. CONCLUSION

This Note demonstrated that under current Supreme Court case law, the Fourth Amendment might extend to the unique Alexa-enabled smart home devices. The Note also demonstrated that the Fourth Amendment's language could, without distortion of its principles, adopt a modern understanding of the term "effects" to encompass the smart device and the data that it transmits.

The Note also discussed digital curtilage, a new framework to constitutionally protect smart devices and the data they emanate from government interception. Although the Supreme Court of the United States has not ruled on the constitutionality of law enforcement's obtaining Alexa-enabled smart home data, the current case law shows that a warrant would be required. Based on the Supreme Court's prior decisions, the Court leaves the door open for developing new theories to adapt to the advancement of technology. The theory of digital curtilage offers society a framework that integrates the nuances of smart technology and the Fourth Amendment.