University of Dayton Law Review

Volume 45 | Number 1 Article 7

1-1-2020

Carpenter v. United States: The Stored Communications Act Is Not a Permissible Mechanism to Obtain Data from Smart Home Devices

Haley Napier
University of Dayton

Follow this and additional works at: https://ecommons.udayton.edu/udlr

 Part of the Law Commons

Recommended Citation
Napier, Haley (2020) "*Carpenter v. United States:* The Stored Communications Act Is Not a Permissible Mechanism to Obtain Data from Smart Home Devices," *University of Dayton Law Review*: Vol. 45: No. 1, Article 7.
Available at: https://ecommons.udayton.edu/udlr/vol45/iss1/7

This Comment is brought to you for free and open access by the School of Law at eCommons. It has been accepted for inclusion in University of Dayton Law Review by an authorized editor of eCommons. For more information, please contact mschlangen1@udayton.edu, ecommons@udayton.edu.

Carpenter v. United States: The Stored Communications Act Is Not a Permissible Mechanism to Obtain Data from Smart Home Devices

Cover Page Footnote

Thank you to my family and friends for their endless support and encouragement throughout my law school experience. I would also like to thank the members of the *University of Dayton Law Review* for making this Comment possible.

This comment is available in University of Dayton Law Review: https://ecommons.udayton.edu/udlr/vol45/iss1/7

CARPENTER V. UNITED STATES: THE STORED COMMUNICATIONS ACT IS NOT A PERMISSIBLE MECHANISM TO OBTAIN DATA FROM SMART HOME DEVICES

*Haley Napier**

I. INTRODUCTION

In 2015, James Bates had friends over to his house to watch a football game.[1] The following morning, Victor Collins was found dead, floating face-down in the hot tub in the backyard.[2] Prosecutors brought charges against Bates for first-degree murder.[3] During the investigation, police discovered an

* J.D. Candidate (expected May 2019) at the University of Dayton School of Law. Thank you to my family and friends for their endless support and encouragement throughout my law school experience. I would also like to thank the members of the University of Dayton Law Review for making this Comment possible.

[1] Colin Dwyer, *Arkansas Prosecutors Drop Murder Case that Hinged on Evidence from Amazon Echo*, NPR (Nov. 29, 2017, 5:27 PM), https://www.npr.org/sections/thetwo-way/2017/11/29/567305812/arkansas-prosecutors-drop-murder-case-that-hinged-on-evidence-from-amazon-echo.

[2] *Id.*

[3] *Id.*

Published by eCommons, 2020

Amazon Echo device in the kitchen.[4] Police seized the Amazon Echo to obtain potential recorded evidence of the murder from the night before.[5] From this device, police were eventually able to determine that there had been "possible cleanup" of the crime.[6] Although the murder charges against Bates were subsequently dropped for various reasons, significant Fourth Amendment issues continued to linger throughout the investigation of the murder, as well as questions regarding the constitutionality of seizing the data from the Amazon Echo.[7]

Smart home devices, such as Amazon Echo, Google Home, and Apple HomePod, are *always* listening.[8] From the most private conversations to the music being played, daily conversations, activities, and personal data are constantly being heard and collected any time these devices believe they hear their "wake words."[9] Although there are many useful features that these smart devices provide to assist in various aspects of daily life—including music playback, voice commands, and acting as a home hub—they also gather personal details about one's life and hear almost anything that is said.[10] While there are big questions of personal privacy violations related to these smart devices, there are even greater questions of whether the government can access the information on these devices for use in criminal prosecutions. If the government is able to obtain this information, issues continue to linger about whether the information can be accessed by a court order issued under the Stored Communications Act or whether a search warrant based on probable cause is required.[11]

The Fourth Amendment governs all searches and seizures conducted by the government.[12] Though not explicitly indicated in the Fourth Amendment's language, its protection against unreasonable searches and seizures encompasses the right of privacy, as provided for in *Katz v. United*

---

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *See* Valentina Palladino, *Guidemaster: Everything Amazon's Alexa Can Do, plus the Best Skills to Enable*, ARS TECHNICA (Dec. 26, 2017, 7:45 AM), https://arstechnica.com/gadgets/2017/12/guidemaster-everything-amazons-alexa-can-do-plus-the-best-skills-to-enable/; Jimmy Westenberg, *The Best Google Home Services You Should Know About*, ANDROID AUTH., https://www.androidauthority.com/google-home-services-749968/ (last visited Feb. 15, 2020); *HomePod*, APPLE, https://www.apple.com/homepod/ (last visited Feb. 15, 2020).

[9] Kim Komando, *When Smart Devices Watch You, What Do They Do with the Data?*, USA TODAY (June 20, 2019, 5:00 AM), https://www.usatoday.com/story/tech/columnist/2019/06/20/what-do-smart-devices-do-data-they-collect-you/1483051001/.

[10] *Id.* (noting that these speaker-activated devices are always listening for their "wake phrases").

[11] Deanna Paul, *The Battle Between Privacy and Law Enforcement Isn't Going Away*, THE GUARDIAN (June 26, 2018, 11:53 AM), https://www.theguardian.com/commentisfree/2018/jun/26/battle-between-privacy-law-enforcement-carpenter.

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

States.[13] Under what is known as the *Katz* reasonable expectation of privacy test, the Fourth Amendment protects those places where: (1) an individual has a subjective expectation of privacy; and (2) society is prepared to recognize that expectation as reasonable.[14] The Fourth Amendment "has long recognized the importance of protecting individuals within their homes from governmental intrusion."[15] Thus, the home is one of the most sacred places that are subject to Fourth Amendment protections under this test.

One exception to the Fourth Amendment's protection against unreasonable searches and seizures is the third-party doctrine, which provides that information voluntarily given to third parties is not protected under the Fourth Amendment.[16] By disclosing information to a third party, an individual loses his Fourth Amendment protections against search and seizure of the information revealed.[17] The Fourth Amendment's protection against unreasonable searches and seizures applies to information for which a person has a reasonable expectation of privacy.[18] Accordingly, under the third-party doctrine, a person does not have a reasonable expectation of privacy to information revealed to a third party.[19] The third-party doctrine essentially "create[s] a privacy gap by denying Fourth Amendment protection to [information] processed by third parties."[20]

Congress responded to the minimal protections of the third-party doctrine by enacting the Stored Communications Act ("SCA").[21] One of the goals of the SCA was to provide increased protection by requiring a court order to obtain certain electronically stored data.[22] The SCA requires no probable cause or warrant to search certain information stored in technological databases.[23] Instead, the SCA permits the government to compel the disclosure of telecommunications when it "offers specific and

---

[13] Justin M. Wolcott, *Criminal Procedure: Are Smartphones Like Footlockers or Crumpled Up Cigarette Packages? Applying the Search Incident to Arrest Doctrine to Smartphones in South Carolina Courts*, 61 S.C. L. REV. 843, 849 (2010) (commenting on the Fourth Amendment's embedded privacy right); *see, e.g.*, Katz v. United States, 389 U.S. 347, 350 (1967); New York v. Class, 475 U.S. 106, 112 (1986); United States v. Miller, 425 U.S. 435, 442 (1976); Smith v. Maryland, 442 U.S. 735, 740 (1979).

[14] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[15] Laura K. Donahue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 560 (2017).

[16] Ryan Watzel, *Riley's Implications for Fourth Amendment Protection in the Cloud*, 124 YALE L.J. F. 73, 74 (2014).

[17] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

[18] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[19] Kerr, *supra* note 17, at 563.

[20] Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 247 (2016).

[21] *See* S. REP. NO. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3556 (acknowledging the minimal privacy protections under existing case law once information has been turned over to a third party and the need to address these privacy concerns); *see generally* 18 U.S.C. § 2703 (2012).

[22] 18 U.S.C. § 2703(d); *see also* S. REP. NO. 99-541, at 5 (noting the Committee's belief that the law "represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies").

[23] 18 U.S.C. § 2703(d).

Published by eCommons, 2020

articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation."[24] Thus, a court order can be issued under the SCA requiring the disclosure of personal information without probable cause.[25]

As new technologies arise, however, questions regarding the Fourth Amendment protections have emerged, especially in regard to what information the government can lawfully obtain from smart home devices.[26] Due to the significant amount of technology, the traditional view regarding the privacy in one's home is severely threatened.[27] Therefore, because of the ample amounts of personal information stored on smart home devices, a court order under the SCA cannot be used to gather this data, and a probable cause warrant under the Fourth Amendment should be issued in order to seize the data on these devices.[28] Without such a requirement, the government would severely intrude on one's Fourth Amendment protections.

This Comment addresses the Fourth Amendment's protection against unreasonable searches and seizures, as well as the privacy of individuals in the ever-growing age of technology. Section II discusses the Fourth Amendment and its impact on smart home devices, as well as the third-party doctrine and the SCA. That section later addresses the recent Supreme Court decision in *Carpenter v. United States* and its holding with regard to cell-site location information ("CSLI"). Section III explores the *Carpenter* decision and why the Court's holding should be extended to governmental seizure of information on smart home devices. That section further considers the impact on the prosecution of crimes if the SCA were a permissible mechanism for gathering data from smart home devices. Finally, Section III compares smart home devices to the CLSI data addressed in *Carpenter* and proposes to use the probable cause standard and warrant requirement, rather than the SCA, to gather data from smart home devices. Section IV provides an overall conclusion to this Comment.

II. BACKGROUND

A. The Fourth Amendment and Smart Homes

The Fourth Amendment to the United States Constitution governs all

---

[24] *Id.*

[25] *See id.*; Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (observing that a showing of "reasonable grounds" under the SCA "falls well short of the probable cause required for a warrant").

[26] *See* Susan W. Brenner, *The Search and Seizure of Computer and Electronic Evidence: The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 50–53 (2005).

[27] Margot E. Kaminski et al., *Symposium Essays from the State of Cyberlaw: Security and Privacy in the Digital Age: Averting Robot Eyes*, 76 MD. L. REV. 983, 984 (2017).

[28] *See* Joel Lee, *How Much of Your Personal Data Could Smart Devices Track?*, MAKE USE OF (Jan. 19, 2016), https://www.makeuseof.com/tag/personal-data-smart-devices-reveal/.

https://ecommons.udayton.edu/udlr/vol45/iss1/7

searches and seizures conducted by the government.[29] The Fourth Amendment provides:

> The 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 particularly describing the place to be searched, and the persons or things to be seized.[30]

The Fourth Amendment contains two clauses: the reasonableness clause and the warrant clause.[31] The reasonableness clause provides that "all government searches and seizures be reasonable."[32] A search occurs when the government intrudes onto private property for the purpose of obtaining information or when it violates a person's legitimate expectation of privacy.[33] "If [a] person [does] not have a reasonable expectation of privacy over [an] area, then the Fourth Amendment and its protections are not even implicated."[34] For instance, there is no expectation of privacy for information accessed and searched by consent.[35] However, without consent, the warrant clause requires probable cause and particularity, which includes "particularized descriptions of the 'place to be searched' and 'the people or things to be seized.'"[36] A probable cause determination for a search warrant generally has two steps.[37] First, the "historical facts" must be considered, including the events and activities leading up to the search.[38] Second, a determination must be made as to "whether [the] historical facts, viewed from the standpoint of an objectively reasonable police officer, amount to . . . probable cause."[39]

A search of someone's information in which they have a reasonable expectation of privacy, such as the interior of their home, is justified *only* upon a showing of probable cause to believe the object is in a certain place, and there must be a "nexus . . . between the item to be seized and [the] criminal

---

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

[30] *Id.*

[31] *See id.*; Kentucky v. King, 131 S. Ct. 1849, 1856 (2011) (stating the Fourth Amendment establishes two requirements).

[32] William Clark, *Protecting the Privacies of Digital Life:* Riley v. California, *the Fourth Amendment's Particularity Requirement, and Search Protocols for Cell Phone Search Warrants*, 56 B.C. L. REV. 1981, 1986 (2015) (citing U.S. CONST. amend. IV); Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (stating that "the ultimate touchstone of the Fourth Amendment is 'reasonableness'").

[33] *See* Oliver v. United States, 466 U.S. 170, 177 (1984).

[34] *See* Wolcott, *supra* note 13, at 849 (citing New York v. Class, 475 U.S. 106, 112 (1986)).

[35] *See, e.g.*, United States v. Cordero-Rosario, 786 F.3d 64, 74 (1st Cir. 2015) (voluntary consent to electronic devices).

[36] *See* Clark, *supra* note 32, at 1986.

[37] Ornelas v. United States, 517 U.S. 690, 696 (1996).

[38] *Id.*

[39] *Id.*

Published by eCommons, 2020

behavior."[40] Probable cause is based on the totality of the circumstances.[41] It is based on probabilities and practical considerations of life "on which reasonable and prudent men . . . act."[42] Under this standard, police must find probable cause that the property contains evidence of criminal activity.[43]

At the time of the adoption of the Fourth Amendment, the Framers could not have envisioned the world of technology we have today. With the advancement of technology and smart home devices, this opens the door for the government to obtain data gathered by these devices, opening a window into a significant portion of one's personal information and data about his or her daily life.[44] As discussed later in Section III, this Comment advises that obtaining the data collected by these devices should constitute a search under the Fourth Amendment.

B. The Third-Party Doctrine

"The third-party doctrine generally holds that a person has 'no legitimate expectation of privacy in'—and therefore no Fourth Amendment protection of—'information he voluntarily turns over to third parties.'"[45] An important implication that arises from this principle is that it "allows the government to collect any information . . . entrusted to a third party without [running] afoul of the Fourth Amendment."[46]

The evolution of the third-party doctrine began with *Katz v. United States* in which the Supreme Court established what is known as the reasonable expectation of privacy test.[47] This test essentially entails two parts: (1) does the person have a subjective expectation of privacy; and (2) is society prepared to accept that expectation of privacy as reasonable.[48] In *Katz*, law enforcement officers attached an eavesdropping device to the outside of a public telephone booth used by the defendant, based on the suspicion that he was transmitting illegal gambling information over the phone.[49] The Supreme Court held that a search of one's property extends to areas where a person has a reasonable expectation of privacy, and therefore wiretapping of telephone calls made from a public telephone booth constitutes a search.[50] Based on the standard enumerated by the Court, the defendant had a

---

[40] Steagald v. United States, 451 U.S. 204, 213 (1981); Warden v. Hayden, 387 U.S. 294, 307 (1967).
[41] Illinois v. Gates, 462 U.S. 213, 233 (1983).
[42] Brinegar v. United States, 338 U.S. 160, 175 (1949).
[43] *See* United States v. Place, 462 U.S. 696, 706 (1983).
[44] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).
[45] Watzel, *supra* note 16, at 74 (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).
[46] Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 985 (2016).
[47] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
[48] *Id.*
[49] *Id.* at 348.
[50] *Id.* at 353.

https://ecommons.udayton.edu/udlr/vol45/iss1/7

reasonable expectation of privacy in the public telephone booth, and thus his conviction was reversed.[51] This was a significant decision by the Supreme Court in that it extended searches and seizures to non-physical intrusions.[52]

Following the decision in *Katz*, the Supreme Court continued to adapt the reasonable expectation of privacy test and created what is now known as the third-party doctrine.[53] In *Couch v. United States*, the Internal Revenue Service issued a subpoena to a restaurant owner's accountant to produce records created for tax preparation purposes.[54] The tax documents were already voluntarily given to the accountant and were no longer possessed by the owner.[55] The Supreme Court held that the restaurant owner did not have a reasonable expectation of privacy in the business records he disclosed to the accountant.[56]

Similarly, in *United States v. Miller*, the Supreme Court found that documents "voluntarily conveyed" to a bank could be shared with the government without a valid search warrant.[57] The defendant was charged with possessing unregistered alcohol distilling equipment and possessing whiskey without having paid the whiskey tax, among other tax fraud.[58] In conducting its investigation, the Bureau of Alcohol, Tobacco, and Firearms issued subpoenas to two of the defendant's bank accounts.[59] The banks disclosed the defendant's records to law enforcement, and he was subsequently convicted.[60] The Court affirmed the defendant's conviction, finding that the documents were not the defendant's private papers because he voluntarily provided them to the bank.[61] In both *Couch* and *Miller*, the Court emphasized the insensitive nature of the information and the fact that the defendants had voluntarily disclosed the information to a third party (i.e., the accountant and the bank).[62]

The Supreme Court created a much more concrete third-party doctrine in *Smith v. Maryland*.[63] In *Smith*, law enforcement officers placed a pen register, a device that only records numbers dialed, on the defendant's telephone after he began making threatening phone calls to the victim of a suspected robbery.[64] The pen register later recorded a call from the defendant

---

[51] *Id.* at 359.
[52] *See id.*
[53] *See* Couch v. United States, 409 U.S. 322, 335–36 (1973).
[54] *Id.* at 324–25.
[55] *See id.* at 324.
[56] *Id.* at 336.
[57] 425 U.S. 435, 442 (1976).
[58] *Id.* at 436.
[59] *Id.* at 437.
[60] *Id.* at 436.
[61] *Id.* at 440.
[62] *Id.* at 444; Couch v. United States, 409 U.S. 322, 335 (1973).
[63] 442 U.S. 735 (1979).
[64] *See id.* at 737.

Published by eCommons, 2020

to the victim, which led to police obtaining a search warrant for the defendant's house.[65] During the search of the house, police discovered a phone book with the corner turned down on the page where the victim's name was found.[66] The defendant was subsequently convicted of robbery.[67] The Supreme Court upheld the defendant's conviction, finding that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[68] Because the defendant "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business[,] . . . he could claim no legitimate expectation of privacy" in the numbers he dialed.[69] Again, the voluntariness of defendant's disclosure and the impersonal information that was disclosed were key to the decision in the case.[70]

The justifications in these decisions could be used to find that individuals enjoy the right to a reasonable expectation of privacy in sensitive and personal information, even when disclosed to third parties. Because Amazon, Google, and Apple are third parties to which users have disclosed personal, sometimes extremely sensitive, information through the use of their smart home hubs, these devices cannot fall within the third-party doctrine. Although these companies are third parties to whom their users voluntarily consent to being recorded and having their data collected, stringent Fourth Amendment search and seizure requirements should be maintained. Furthermore, with the increasing use of these smart home devices and the number of households that use them in their daily lives, the warrant requirement should be strictly followed in order to protect against unreasonable acquisition of someone's most private details and conversations.

C. The Stored Communications Act

The SCA, as amended in 1994, provides safeguards to "certain electronic communications but also preserves avenues for law enforcement to effectively conduct criminal investigations."[71] The SCA protects electronic communications in three important ways:

> (1) [I]t provides a private cause of action against anyone who

---

[65] *Id.*
[66] *Id.*
[67] *Id.* at 738.
[68] *Id.* at 743–44.
[69] *Id.* at 744.
[70] *See id.* at 745.
[71] Melissa Medina, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U. L. REV. 267, 276 (2013) (explaining that the SCA protects electronic communications by providing a private cause of action against anyone who acquires stored communications and regulating when service providers can disclose user information).

https://ecommons.udayton.edu/udlr/vol45/iss1/7

> intentionally "obtains, alters, or prevents authorized access" to certain stored communications; (2) it regulates when network service providers may voluntarily disclose customer communications and records; and (3) it outlines specific rules that govern when state actors may compel disclosure of stored communications from network service providers.[72]

Under the SCA, there are two primary uses of computer networks that Congress sought to regulate: "(1) electronic communication services (ECS) designed to handle 'data transmissions and electronic mail' and (2) remote computing services (RCS) intended to provide outsourced computer processing and data storage."[73]

In order to qualify as ECS communication, first, the service provider must offer users "the ability to send or receive . . . electronic communications."[74] Electronic communications encompass "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part[] by a wire, radio, electromagnetic, photoelectronic or photooptical system."[75] Second, the service provider must hold the electronic communication in "electronic storage."[76]

Congress created the category of RCS to address third-party service providers.[77] A third-party service provider must meet four requirements to qualify as a RCS:

> First, the provider must offer "computer storage or processing services" to the public through an electronic communications system. Second, the data must be received electronically from the customer. Third, the content must be "carried or maintained" by the service provider "solely for the purpose of providing storage or computer processing services" to the customer. Finally, the provider cannot be "authorized to access the [customer's] content for purposes of providing any services other than storage or computer processing."[78]

The SCA permits the government to compel the disclosure of certain telecommunications, those that qualify as RCS, when it "offers specific and

---

[72] *Id.* at 269.

[73] William Jeremy Robison, *Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1205 (2010) (citing H.R. REP. NO. 99-647, at 21, 23 (2001)).

[74] *Id.* at 1206 (citing 18 U.S.C. § 2510(15) (2012)).

[75] Allegra Bianchini, Note, *Always On, Always Listening: Navigating Fourth Amendment Rights in a Smart Home*, 86 GEO. WASH. L. REV. ARGUENDO 1, 17 (2018).

[76] Robison, *supra* note 73, at 1206.

[77] *See* S. REP. NO. 99-541, at 10–11 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3556.

[78] Robison, *supra* note 73, at 1207 (internal footnotes omitted).

Published by eCommons, 2020

articulable facts showing that there are reasonable grounds to believe that the . . . records . . . sought, are relevant and material to an ongoing criminal investigation."[79] Smart home devices can be considered RCS communication because they are a third-party provider that stores electronic content for the consumer.[80] For this reason, these devices and the data contained within them receive fewer privacy protections.[81] Therefore, all that is needed under the SCA to obtain personal data from smart home devices is "reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation"—a standard much lower than probable cause for a search warrant.[82]

D. Carpenter v. United States

In *Carpenter v. United States*, police officers arrested four men suspected of committing a series of bank robberies at various Radio Shack and T-Mobile stores.[83] One suspect confessed and later identified fifteen accomplices who participated in the robberies.[84] The suspect also gave Federal Bureau of Investigation agents some of the accomplices' cell phone numbers, upon which the agents reviewed the records to identify additional telephone numbers that were called around the time the robberies occurred.[85] Based on this information, prosecutors sought a court order under the SCA to obtain the cell phone records of Carpenter and several others suspected to be involved.[86] The order disclosed CSLI for Carpenter's cell phone at the call origination and termination points during the four-month period when the robberies occurred.[87] Altogether, the government obtained 12,898 location points cataloging Carpenter's movements.[88] Based on these data points, the government was able to place Carpenter at almost the exact locations of the robberies.[89] Carpenter was subsequently convicted for the robberies, and the Court of Appeals for the Sixth Circuit affirmed.[90]

---

[79] 18 U.S.C. § 2703(d).

[80] Smart home devices can be considered RCS communication because smart devices contain user data that is stored by the third-party provider. The third-party provider stores that data within the smart device.

[81] Robison, *supra* note 73, at 1208.

[82] 18 U.S.C. § 2703(d); Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018); *see supra* note 25.

[83] 138 S. Ct. at 2212.

[84] *Id.*

[85] *Id.*

[86] *Id.*

[87] *Id.* "Cell phones continuously scan . . . for the best signal, which comes from the closest cell site. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information." *Id.* at 2211. With this information, the general location of cell phone calls can be traced. *Id.*

[88] *Id.* at 2212.

[89] *Id.* at 2213.

[90] *Id.*

https://ecommons.udayton.edu/udlr/vol45/iss1/7

The Supreme Court reversed Carpenter's conviction.[91] The Court suggested a multifactor analysis to determine the private nature of the types of electronic data.[92] This analysis included five factors: (1) "intimacy"; (2) "comprehensiveness"; (3) "expense"; (4) "retrospectivity"; and (5) "voluntariness."[93] Using these factors, the Court determined that the acquisition of Carpenter's CSLI was a search within the Fourth Amendment; therefore, the government needed a warrant supported by probable cause to obtain such data.[94] The Court recognized that the acquisition of CSLI records—which reveal the location of someone whenever a phone call is made or received—does not fit neatly under existing precedents.[95] The Court thus addressed the new phenomenon of how to apply the Fourth Amendment to the ability to chronicle a person's past movement through the record of his cell phone signals.[96]

The Court acknowledged the unique and personal nature of cell-site data.[97] CSLI data is "detailed, encyclopedic, and effortlessly compiled."[98] This data provides a retrospective view of a person's whereabouts, allowing the government to go back in time and retrace activities.[99] It essentially provides an "intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations."[100] Because of the type of information that can be gathered from CSLI data, the Court held that an "individual maintains a legitimate expectation of privacy in the record of his physical movements" captured through cell phone signals.[101]

The Court further addressed CSLI data in relation to the current third-party doctrine.[102] This type of information is not limited to impersonal information—it is a chronicle of location information.[103] CSLI data is not a traditional "business record" for the purposes of the third-party doctrine.[104] It is an entirely different type of record.[105] Although this data is technically disclosed to a third-party wireless carrier, "[m]apping a cell phone's location over [a period of time] provides an all-encompassing record of the holder's

---

[91] *Id.* at 2223.
[92] *Id.* at 2234 (Kennedy, J., dissent) (analyzing the multifactor analysis used by the majority).
[93] *Id.*
[94] *Id.* at 2223.
[95] *Id.* at 2214.
[96] *Id.* at 2216.
[97] *See id.*
[98] *Id.*
[99] *Id.* at 2218.
[100] *Id.* at 2217 (internal quotations omitted).
[101] *Id.*
[102] *See id.* at 2216.
[103] *Id.* at 2219.
[104] *Id.*
[105] *Id.*

Published by eCommons, 2020

whereabouts."[106] Furthermore, a cell phone logs CSLI simply by virtue of its operation; the user does not have to do anything other than power up the device.[107] Thus, location information is not truly "shared" or "voluntarily given" to a third party.[108] In fact, almost everyone has a cell phone, and they have become an indispensable part of modern society.[109] Therefore, giving location data to the cell phone carrier is not really "voluntarily" disclosed within the meaning of the third-party doctrine.[110]

The Court held that "when the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements."[111] Due to the unique nature of cell phone location information and the fact that the data is not truly disclosed to a third party, the government's acquisition of Carpenter's cell-site records was a search within the meaning of the Fourth Amendment.[112] The Court further held that the SCA is an impermissible mechanism to obtain CSLI data, and the data must be obtained with a warrant supported by probable cause.[113] The Court "decline[d] to grant the state unrestricted access to a wireless carrier's database of physical location information."[114] The Court recognized that the state of technology and the accuracy of CSLI data are rapidly increasing, providing law enforcement a "powerful new tool" that runs the risk of government encroachment.[115]

E. Smart Home Technology[116]

A smart home is a dwelling that connects electrical appliances, technology devices, and other services through a communications network, which allows them to be remotely accessed, monitored, and controlled.[117] "Smart home technology . . . provides homeowners security, comfort, convenience and energy efficiency by allowing them to control smart devices . . . ."[118] In order to reach a unified home monitoring system, the smart devices "must possess sensing, data processing, and wireless communication

---

[106] *Id.* at 2217.
[107] *Id.* at 2220.
[108] *Id.*
[109] *See id.*; *see also Mobile Fact Sheet*, PEW RESEARCH CTR.: INTERNET AND TECH. (June 12, 2019), http://www.pewinternet.org/fact-sheet/mobile/ (96% of Americans own a cell phone of some kind).
[110] *Carpenter*, 138 S. Ct. at 2220.
[111] *Id.* at 2219.
[112] *Id.* at 2220.
[113] *Id.* at 2221.
[114] *Id.* at 2223.
[115] *Id.* at 2223.
[116] The scope of this Comment is limited to analyzing speaker-activated smart home devices, such as the Amazon Echo, Google Home, and Apple HomePod.
[117] *What is a "Smart Home"?*, SMART HOME ENERGY, http://smarthomeenergy.co.uk/what-smart-home (last visited Feb. 15, 2020).
[118] Margaret Rouse, *Smart Home or Building (Home Automation or Domotics)*, IOT AGENDA, http://internetofthingsagenda.techtarget.com/definition/smart-home-or-building (last visited Feb. 15, 2020).

https://ecommons.udayton.edu/udlr/vol45/iss1/7

functions."[119] With these features, a smart home is capable of creating an easier lifestyle and a more operational household. With the proper devices, virtually everything could be automated and controlled through smart technology.[120]

Smart technology, such as phones or computers, has been advancing for decades, but only recently have homes begun incorporating smart technologies.[121] Today, the number of smart home devices is rapidly increasing.[122] The first smart phone was introduced in 1992.[123] Over a decade later, in January 2007, the Apple iPhone was released.[124] Soon after, Google introduced its version of the smart phone, the Android.[125] Over the next few years, different companies introduced various advancements to smart devices.[126] Such advancements included iPads, tablets, laptops, and smart televisions.[127] The most recent of these advancements in smart technology today, however, include Amazon Echo, Google Home, and Apple HomePod.[128] These devices allow for a digitally connected world at the touch of a hand or the sound of a voice to provide a better quality of living through home networking.[129]

Amazon Echo, Google Home, and Apple HomePod are hands-free, smart speaker devices connected to voice-controlled personal assistants.[130]

---

[119] *What is a Smart Home?*, VIVINT SMARTHOME (July 26, 2015), https://www.vivint.com/resources/article/what-is-a-smart-home.

[120] *See 9 Smart Home Devices that Automate Your Home*, NATIONWIDE (Sept. 30, 2019), https://blog.nationwide.com/9-wifi-home-automation-apps/.

[121] *See* Lindsay Rothfeld, *Tech Time Machine: The Smart Home*, MASHABLE, https://mashable.com/2015/01/08/smart-home-tech-ces/ (last visited Feb. 15, 2020).

[122] *Id.*

[123] Steven Tweedie, *The World's First Smartphone, Simon, Was Created Years Before the iPhone*, BUS. INSIDER (June 14, 2015, 8:00 AM), http://www.businessinsider.com/worlds-first-smartphone-simon-launched-before-iphone-2015-6.

[124] Charles Arthur, *The History of Smartphones: Timelines*, THE GUARDIAN (Jan. 24, 2012, 3:00 PM) https://www.theguardian.com/technology/2012/jan/24/smartphones-timeline.

[125] *Id.*

[126] *See* Julie Bort, *The History of the Tablet, an Idea Steve Jobs Stole And Turned Into a Game-Changer*, BUS. INSIDER (June 2, 2013, 8:00 AM), https://www.businessinsider.com/history-of-the-tablet-2013-5.

[127] *See, e.g.*, *id.*; Mark J. Perry, *Technology Has Advanced so Rapidly That a Laptop Computer Today is 96% Cheaper than a 1994 Model and 1,000X Better*, AEI (May 25, 2016), https://www.aei.org/carpe-diem/technology-has-advanced-so-rapidly-that-a-laptop-computer-today-is-96-cheaper-than-a-1994-model-and-1000x-better/; *Advancements of TV Technology*, PALMGEAR (July 2, 2015), https://www.palmgear.com/2015/02/07/advancements-of-tv-technology/.

[128] *See generally HomePod*, MACRUMORS, https://www.macrumors.com/roundup/homepod/ (last visited Feb. 15, 2020); Andrew Gebhart, *Google Home's 2017 in Review: All Grown Up and Ready to Battle*, CNET (Dec. 20, 2017, 12:00 PM), https://www.cnet.com/news/google-homes-year-in-review-all-grown-up-and-ready-to-battle/; Brandon Vigliarolo, *Amazon Alexa: Cheat Sheet*, TECHREPUBLIC (Sept. 27, 2019, 6:27 AM), https://www.techrepublic.com/article/amazon-alexa-the-smart-persons-guide/.

[129] Ben King, *On the Internet of Things, More Devices are Becoming Smart and Connected – What's that Mean?*, SINGULARITY U. (Oct. 15, 2018), https://su.org/blog/on-the-internet-of-things-more-devices-are-becoming-smart-and-connected-whats-that-mean/.

[130] *See Set Up Your Amazon Echo*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201601770 (last visited Feb. 15, 2020); GOOGLE NEST HELP, https://support.google.com/google

Published by eCommons, 2020

These devices assist in the management and control of one's lifestyle simply by the sound of their voice.[131] Each of these devices are capable of voice interaction, music playback, providing weather and news alerts, sending messages and receiving phone calls, and act as a home automation hub for all smart devices.[132] With these services, smart home devices create a more functional household, enabling owners to handle everyday tasks more easily.

Although smart home automation devices create a more controlled, manageable, and operational household, they also pose many different privacy and security risks.[133] The Federal Trade Commission has indicated various security risks that could be exploited by: "(1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating risks to personal safety."[134] Amazon Echo, Google Home, and Apple HomePod are capable of storing personal information, records of daily communication, user habits, geographical locations, financial data, and other similar information that is vulnerable to security and privacy attacks.[135]

Perhaps one of the biggest privacy factors is the continuous "eavesdrop[ping]" by the third-party manufacturer or other intruder into a private home.[136] Third parties are able to gather data about users when these devices record such information.[137] Although Amazon, Google, and Apple all have user privacy agreements, consumers remain concerned about the ability of their information to be collected, saved, and potentially released impermissibly, especially to a governmental agency.[138] These devices

---

home/answer/7071994 (last visited Feb. 15, 2020); *HomePod*, *supra* note 8; *HomePod: Everything You Need to Know About Apple's Smart Speaker*, MACWORLD (Sept. 12, 2018), https://www.macworld.com/article/1030983/home-tech/homepod.html.

[131] *See, e.g.*, *HomePod*, *supra* note 8; Don Reisinger, *What is Google Home? We Explain Google's Smart Home Platform*, TOM'S GUIDE (Oct. 26, 2016), https://www.tomsguide.com/us/google-home-faq,review-3976.html; Palladino, *supra* note 8.

[132] *See* Palladino, *supra* note 8; Westenberg, *supra* note 8; *HomePod*, *supra* note 8.

[133] *See Know the Risks of Amazon Alexa and Google Home*, NAKED SECURITY (Jan. 27, 2017), https://nakedsecurity.sophos.com/2017/01/27/data-privacy-day-know-the-risks-of-amazon-alexa-and-google-home.

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

[135] *Id.*

[136] *Id.* at 17.

[137] *See What is a Smart Speaker: How Do Smart Speakers Work*, ELEC. NOTES, https://www.electronics-notes.com/articles/equipment-items-gadgets/smart-home/what-is-smart-speaker.php (last visited Feb. 15, 2020). For example, with the Amazon Echo, once the system hears the word to activate the speaker, it records what is being said and sends it over the Internet to the main processing area or voice recognition service. *Id.* For the Amazon system, the speech file is sent to Amazon's Alexa Voice Services in the cloud. *Id.*

[138] *See generally Amazon Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496 (last updated Jan. 1, 2020); *Apple Privacy Policy*, APPLE, https://www.apple.com/legal/privacy/en-ww/ (last updated Dec. 31, 2019); *Google Privacy Policy*, GOOGLE, https://www.google.com/policies/privacy/ (last updated Dec. 19, 2019); *see* Jason Knowles and Anne Pistone, *Who is Listening? Smart Hub Devices Spark Privacy Concerns*, ABC7 CHICAGO (Feb. 13, 2017), http://abc7chic

essentially allow for endless unpermitted intrusions into one's personal privacy.[139]

III. ANALYSIS

A. Smart home devices provide an "intimate window into [one's personal] life"[140]

As with GPS data and CSLI data, the data gathered from smart home devices provides an "intimate window into [one's personal] life."[141] Not only are smart home devices capable of creating a more automated and controlled lifestyle, these devices also track the user's activities, music playlists, recent purchases, Internet searches, news information, and phone calls and text messages.[142] On a more personal matter, when the capability is enabled, smart home devices can even record users' communications and conversations.[143] Time-stamped data, much like the data collected on smart home devices, reveals a person's particular movements, thereby further revealing his familial, political, professional, religious, and sexual associations.[144] This information can provide details of a person's hobbies, personal views, attitudes, and beliefs about a variety of different topics. These devices provide an exhaustive chronicle of personal information from the time a person purchases the smart device and turns it on, until the time that it is turned off.[145] They provide a detailed log of activities and track every moment of every day.[146] CSLI data, in comparison, tracks a cell phone user's location whenever he has the phone on his person.[147] Because smart home devices are located throughout one's home, they are essentially part of that person's home, and the user has sought to keep this information to himself, within his home. Thus, the person has a reasonable expectation of privacy in the data collected on those devices. Smart home devices hold the privacies of one's life, and therefore, the expectation of privacy in data collected on smart home devices should be recognized as reasonable.

Using the same multi-factor analysis recognized by the Supreme Court in *Carpenter*, it is clear that smart home device data is much more

---

ago.com/technology/who-is-listening-smart-hub-devices-spark-privacy-concerns/1753155/.

[139] The Author believes that, despite agreeing to user privacy agreements, third-party providers have unlimited access to personal information. While one would hope their personal data is not being used incorrectly, there is no way of knowing how much one's personal information is being used.

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

[141] *Id.*

[142] The basis of this information is the Author's own personal knowledge from using smart home devices.

[143] *See supra* Section II.E.

[144] United States v. Jones, 565 U.S. 400, 415 (2012).

[145] *Carpenter*, 138 S. Ct. at 2219.

[146] *Id.* at 2218.

[147] *Id.* at 2211.

Published by eCommons, 2020

personal than CSLI data.[148] First, smart home data is extremely intimate and personal.[149] Smart home devices essentially record one's life and the activities conducted within the residence.[150] The home is considered to be where a person has the highest expectation of privacy.[151] For this reason, people seek to preserve the activities within their home as private. However, with smart devices, the government can "go inside" one's home and gather information about people that would otherwise never be heard or known.[152] The government can use smart home devices as a surveillance tool, essentially allowing the government to see one's affairs within the confines of their home.[153]

Second, smart home devices provide a comprehensive image of users' hobbies, activities, and conversations.[154] Smart home devices provide a complete and accurate record of all aspects of one's life while in their home.[155] These devices are capable of recording what type of music is being played; what the user searches on the Internet; what a user says in conversation; and even when the user is physically at home.[156] These devices store financial information, as well as credit card numbers and recent purchases.[157] Smart home devices collect a wide range of personal information that the user intends to be kept secret and away from the government.[158]

Third, home smart devices record all past conversations and activities, essentially allowing the government to look into someone's past, which it would be unable to do without the device.[159] Smart home devices are retrospective.[160] Users could normally proceed with their daily activities and conversations without anyone ever knowing the details of those activities or conversations. However, with the capabilities of these devices, the government is able to go back in time and see *the entire* user's past

---

[148] *See, e.g., id.*

[149] *See* Geoffrey A. Fowler, *Alexa Has Been Eavesdropping on You This Whole Time*, WASH. POST (May 6, 2019, 9:00 AM), https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/.

[150] *See, e.g., id.*

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

[152] Trevor Timm, *The Government Just Admitted It Will Use Smart Home Devices For Spying*, THE GUARDIAN (Feb. 9, 2016, 3:29 PM), https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government.

[153] *Id.*

[154] *See* Arushi Lohia, *Be Warned! Your Smart Devices Are Actually Listening to & Recording Everything You're Saying*, SCOOP WHOOP (Jan. 4, 2018, 2:07 PM), https://www.scoopwhoop.com/smart-devices-are-actually-recording-everything-youre-saying/.

[155] *See id.*

[156] *See* Fowler, *supra* note 149.

[157] *See* Latoya Irby, *7 Tips for Making Safe Mobile Payments*, THE BALANCE, https://www.thebalance.com/tips-for-safe-mobile-payments-4137835 (last updated July 29, 2019).

[158] *See* Fowler, *supra* note 149.

[159] *See id.*

[160] *Id.*

conversations and activities.[161]

Finally, users of smart home devices are not voluntarily giving up their private information in the usual sense. Although the user consents for the company to have their data, the data is not revealed voluntarily for use in any type of investigation.[162] By using a smart home device, the device's company is able to get data from the device.[163] However, the companies use the information for business and marketing purposes and essentially for ensuring proper operation and functionality of the devices.[164] On the other hand, the government is using the data to track one's life and activities in order to investigate a potential crime.[165] Users do not voluntarily turn over every aspect of their life to help in an investigation, nor do they voluntarily give the government "near perfect surveillance" over their lives.[166] This is exactly what smart home devices would provide to the government—an "intimate window into [one's] life."[167]

B. Smart home devices do not fall under the traditional definition of the third-party doctrine

Smart home devices do not fall under the traditional meaning of the third-party doctrine.[168] The third-party doctrine provides that a person has no reasonable expectation of privacy in information conveyed to third parties.[169] Although information stored on smart home devices is technically given to a third party, such as Amazon, Google, Apple, or a similar company, under the third-party doctrine, this is *just different*, as was the CSLI data obtained in *Carpenter*.[170] The Court in *Carpenter* declined to extend the third-party doctrine to CSLI data.[171] It held that these records are unique in that they create time-stamps in order to track a person's every location.[172] Just like cell-site data, smart home devices have an infinite number of capabilities that obtain copious amounts of very personal data, including intimate

---

[161] *Id.*

[162] *See* Rebecca Levin, *"Alexa, Can You Keep a Secret?" An Analysis of 4th Amendment Protection Regarding Smart Home Devices*, U. ILL. (Feb. 18, 2019), http://illinoisjltp.com/timelytech/alexa-can-you-keep-a-secret-an-analysis-of-4th-amendment-protection-regarding-smart-home-devices/.

[163] *See, e.g.*, *Amazon Privacy Notice*, *supra* note 138.

[164] *Id.*

[165] *See* Fowler, *supra* note 149.

[166] Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018).

[167] *Id.* at 2217.

[168] *See* Levin, *supra* note 162 (arguing that, in light of *Carpenter*, "smart home device information should be afforded the same protection as cell phone location data and the Third-Party Doctrine should also not apply in the case of smart home devices").

[169] *See supra* Section II.B.

[170] *See* 138 S. Ct. at 2220. By using smart home devices, the user agrees to allow the third-party provider, for example, Amazon, Google, or Apple, to record and store their personal information. *See Amazon Privacy Notice*, *supra* note 138; *Google Privacy Policy*, *supra* note 138; *Apple Privacy Policy*, *supra* note 138.

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

[172] *Id.*

Published by eCommons, 2020

conversations.[173]

In fact, smart home devices contain even more personal and unique data than CSLI.[174] Smart home devices can track Internet history, call information, financial data, such as purchase records and credit card numbers, and daily conversations.[175] Although CSLI data can essentially track one's location, that is all it can do.[176] These data points can be used as circumstantial evidence of one's activities.[177] However, they do not provide an exact record of one's activities like smart home devices do.[178] Smart home devices hold "the privacies of life" and are capable of recording nearly *every* conversation when the device believes it hears its "wake word."[179] By the government seizing this data, it is essentially going into one's home and gathering the most intimate details about one's life, not just the person's location. When viewing the sensitive nature of the data on smart home devices, it is nearly impossible to come to the conclusion that the SCA could be used by the government to obtain this information without probable cause and a warrant. Because a court order under the SCA was not a permissible mechanism to obtain CSLI data in *Carpenter*, and considering how much more private smart home devices are, a court order under the SCA should not be permissible to obtain this data either.[180]

The mere fact that smart home devices contain personal user information that is provided to the third party "owner" of the devices (Amazon, Apple, Google, etc.) cannot overcome the user's claim to Fourth

---

[173] *See* Fowler, *supra* note 149.

[174] *See* Ryan G. Bishop, Note, *The Walls Have Ears . . . and Eyes . . . and Noses: Home Smart Devices and the Fourth Amendment*, 61 ARIZ. L. REV. 667, 688–89 (2019).

[175] *See* Marc Saltzman, *What is a Smart Speaker?*, AARP (Oct. 11, 2019), https://www.aarp.org/home-family/personal-technology/info-2019/smart-speaker-uses.html; Gerald Lynch, *10 Reasons You Need a Smart Speaker*, REAL HOMES (Jan. 7, 2020), https://www.realhomes.com/advice/10-reasons-why-you-need-smart-audio.

[176] Stephanie Lacambra, *Cell Phone Location Tracking or CSLI: A Guide for Criminal Defense Attorneys*, ELEC. FRONTIER FOUND., https://www.eff.org/files/2017/10/30/cell_phone_location_information_one_pager_0.pdf (last visited Feb. 15, 2020).

[177] *See* Bishop, *supra* note 174.

[178] *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018); *see also* Lacambra, *supra* note 176. CLSI data only provides pinpoints of the user's location. *Carpenter*, 138 S. Ct. at 2218. CSLI does not track or record conversations and activities on the cell phone, rather, CLSI only tracks the location of the user. *Id.* As indicated in this Comment, smart devices are able to record conversations, as well as track the user's messages, music playlists, Internet searches, and other personal information. *See supra* Section III.A.

[179] Riley v. California, 134 S. Ct. 2473, 2495 (2014) (observing that "[m]odern 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.'"); *see also* Fowler, *supra* note 149; David Nield, *Your Smart Speakers Are Listening to You. Here's How to Delete Their Recordings*, POPULAR SCI. (June 10, 2018), https://www.popsci.com/delete-smart-speaker-recordings/; *Smart Speaker Recordings Reviewed by Humans*, BBC (Apr. 11, 2019), https://www.bbc.com/news/technology-47893082.

[180] *Carpenter*, 138 S. Ct. at 2221; *see Who Has Access to Your Smart Home?*, INT'L ASS'N OF CHIEFS OF POLICE, https://www.iacpcybercenter.org/whats-new/smart-home-security/ (last visited Feb. 15, 2020).

https://ecommons.udayton.edu/udlr/vol45/iss1/7

Amendment privileges.[181] In addition, based on the user's guide in regards to smart home data turned over to police, the user does not assume the risk that it will be provided to police, absent a valid warrant, just like a cell phone user does not assume the risk that police will use CSLI data to track his daily whereabouts.[182] Just because a smart device user has chosen to use this technology in his daily routine does not mean that he has chosen to provide all his private affairs to a third party. Although some may consider this data business records, it certainly is not. The data is private information about one's life. In determining whether a smart home device should fall within the traditional third-party doctrine, it is important to balance the privacy interests compared to third-party disclosure. In the case of smart home devices, the privacy interests are significantly greater than the sole fact that the personal information was "voluntarily shared" to a third party.

By obtaining information from smart home devices, the government can track everything the user has done.[183] These devices provide a narrative of the user's past activities, Internet searches, conversations, and purchases, just to name a few.[184] The vast amount of information stored on smart devices creates a timeline of when someone conducts activities, when they are at home using the device, and what they are doing in relation to the device.[185] This is exactly like the CSLI data collected in *Carpenter*.[186] By using CSLI data, the government was able to place Carpenter right where the robberies occurred.[187] By obtaining data from smart home devices, the government can, again, place a user at the location of their home at an exact time.[188] As indicated in *Carpenter*, there just cannot be a 24-hour tracking system of one's life and activities.[189] This is what smart home devices do.[190] They are capable of providing a past image of what someone was doing and the details of the conversations he or she was having if the device's "wake word" was

---

[181] *See generally Apple Privacy Policy*, *supra* note 138; *Amazon Privacy Notice*, *supra* note 138; *Google Privacy Policy*, *supra* note 138; *see also supra* notes 166–177 and accompanying text.

[182] *See Carpenter*, 138 S. Ct. at 2220; Bishop, *supra* note 174; *see also Apple Privacy Policy*, *supra* note 138; *Amazon Privacy Notice*, *supra* note 138; *Google Privacy Policy*, *supra* note 138.

[183] *See* Levin, *supra* note 162.

[184] *See* Adrienne Kitchen, *Smart Devices and Criminal Investigations: Protecting Suspects' Privacy and Fourth Amendment Rights*, 54 CRIM. L. BULL. 1, 5–6 (2017).

[185] *See* Donald L. Crowell III, Note, *The Privacy of "Things": How the Stored Communications Act Has Been Outsmarted by Smart Technology*, 70 FED. COMM. L. J. 211, 214 (2018).

[186] *See Carpenter*, 138 S. Ct. at 2220.

[187] *Id.* at 2213.

[188] *See* Fowler, *supra* note 149.

[189] *Compare Carpenter*, 138 S. Ct. at 2220, *with* United States v. Knotts, 460 U.S. 276, 284–85 (1983) (holding that visual surveillance did not constitute a search because the beeper was for "limited use") *and* United States v. Jones, 565 U.S. 400, 430–31 (2012) (finding that longer GPS monitoring tracks "every movement," and therefore constitutes a search under the Fourth Amendment).

[190] The Author believes that smart home devices are a way to track the user's life and activities. As noted in this Comment, smart home devices capture data that records conversations, saves texts messages from connected devices, tracks music playlists, Internet searches, and other personal activities. *See supra* Section III.A. Smart home devices are able to be connected to other smart devices, thereby creating a blueprint of the user's entire life.

Published by eCommons, 2020

triggered.[191] With this data, the government may be able to look back and determine when someone was home, what activities he or she was doing while there, and the conversations they were having.[192] A 24-hour tracking system on someone's home life violates every aspect of privacy that the Fourth Amendment was intended to protect.[193]

C. A court order issued under the SCA does not provide adequate protection of one's personal data on smart home devices

A court order issued under the SCA does not provide adequate protection of one's personal data on smart home devices.[194] Under the SCA, the Government only needs "reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation."[195] The Supreme Court has used the phrase "reasonable grounds to believe" interchangeably with the phrase "reasonable belief."[196] "Reasonable belief" is what "an ordinarily prudent man might be able to assign a just and fair reason for."[197] Thus, the standard for obtaining information on smart home devices is very low considering the amount and type of information being sought.[198] Because the standard for obtaining a court order under the SCA is so low, the government can essentially access all the stored information on these devices as long as it is "relevant and material to an ongoing investigation."[199] By using the SCA, the government could capitalize on the fact that only "reasonable grounds to believe" is necessary to search smart home devices, thereby allowing the government to obtain information that would exceed the scope of a valid search under the Fourth Amendment.[200] "So long as [the data] collection is lawful," as it would be under the SCA, "the Fourth Amendment has nothing to say about how information is

---

[191] *See* Fowler, *supra* note 149; John Kruzel, *Is Your Amazon Alexa Spying on You?*, POLITIFACT (May 31, 2018), https://www.politifact.com/factchecks/2018/may/31/ro-khanna/your-amazon-alexa-spying-you/. The Author notes that smart home devices are always listening to conversations because they are constantly searching for the "wake word." Fowler, *supra* note 149. If these devices were not always listening, they would never be able to hear when the "wake" word is said. *Id.* Even still, sometimes smart home devices misinterpret the "wake" word and record conversations that were never intended to be recorded by the user. *Id.* Because of this, the Author believes that smart home devices are capable of creating a past image of one's life and conversations.

[192] *See id.*

[193] *See Carpenter*, 138 S. Ct. at 2217–18.

[194] *See* Bianchini, *supra* note 75, at 24.

[195] *See supra* Section II.C.

[196] *See e.g.*, Terry v. Ohio, 392 U.S. 1 (1968) (using the phrases "reasonable belief" and "reasonable grounds to believe" interchangeably throughout the opinion).

[197] Garrison v. Louisiana, 379 U.S. 64, 79 (1964). *See, e.g.*, Hiibel v. Sixth Judicial Dist. Ct., 542 U.S. 177, 190–91 (2004); Maryland v. Buie, 494 U.S. 325, 327 (1990); Michigan v. Long, 463 U.S. 1032, 1049 (1983).

[198] Bianchini, *supra* note 75, at 24.

[199] *See Carpenter*, 138 S. Ct. at 2217–18; 18 U.S.C. 2703(d) (2012).

[200] *See id.* at 2221.

employed."[201] Smart home devices, like cell phones, have an immense storage capacity and are capable of capturing large amounts of personal data.[202] As with many of the devices that we have in the age of technology, the data on smart home devices is "detailed, encyclopedic, and effortlessly compiled."[203] As noted in *Carpenter*, the retrospective quality of the CSLI data gives police access to a category of information otherwise unknowable.[204] Data on smart home devices is *very* much the same. Using these devices, the government would be able to travel back in time and recreate a person's activities, conversations, when he is at his residence, Internet searches, items purchased on the device, recent music, and much more.[205] For this reason, a court order issued under the SCA is an impermissible mechanism to obtain this information. The SCA does not provide adequate protections to a user's expectation of privacy.

The Court in *Carpenter* makes note of the government's subpoena power.[206] Under the SCA, the government would be overreaching the scope of its power through the subpoena process.[207] By subpoenaing someone to disclose the data on his or her smart home device, the government would be circumventing the more stringent probable cause requirement for a warrant, and even obtaining the same exact information it would under a warrant using only "reasonable suspicion" for a subpoena.[208] Because of the sensitive nature of the type of information stored on smart home devices, the government should not be able to compel a user to turn over such personal and private information for unlimited access and use by the government.[209] Although the SCA is intended for use only to assist in an ongoing criminal investigation, once the data is disclosed, there is really no way of knowing for what other purposes the government might be using this information.[210] Because the SCA is capable of providing access to a wealth of the most private information about someone, the subpoena power under the SCA needs restrictions for what the government is able to access.[211]

D. A warrant supported by probable cause should be issued to gather

---

[201] Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 578 (2017).

[202] *See* Riley v. California, 573 U.S. 373, 393 (2014) (acknowledging that the cell phones are capable of ample storage of information).

[203] *Carpenter*, 138 S. Ct. at 2209.

[204] *Id.* at 2218.

[205] *See* Fowler, *supra* note 149.

[206] *Carpenter*, 138 S. Ct. at 2221–22.

[207] *Id.* at 2221.

[208] *See* 18 U.S.C. § 2703(d) (2012); *Carpenter*, 138 S. Ct. at 2221.

[209] *See Know the Risks of Amazon Alexa and Google Home*, *supra* note 133; Lohia, *supra* note 154.

[210] *See* 18 U.S.C. § 2703(d).

[211] *See id.*; *Carpenter*, 138 S. Ct. at 2221.

Published by eCommons, 2020

information from smart home devices

A warrant supported by probable cause should be issued to gather information from smart home devices. The basic purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[212] When an individual "'seeks to preserve something as private,'" and his "expectation of privacy is 'one that society is prepared to recognize as reasonable,'" the Court has held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause.[213] Smart home devices are meant to be private. They are within the confines of the user's home. There is no doubt that there is a reasonable expectation of privacy in these devices and what is stored on them. Given the state of current case law, the government could gather this highly personal data gathered by smart home devices using the SCA without running afoul of the Fourth Amendment.[214] The only practical way to escape this reality would be to stay away from smart home devices, and keep them out of one's home.

In order for a search warrant to be issued, there must be particularity in what is being searched or seized.[215] Because of the particularity requirement of a search warrant, there is no blanket permission to search whatever the government desires.[216] They are restricted to the confines of what is allowed in the warrant.[217] However, this aspect of particularity is not required under the SCA.[218] The "reasonable grounds" standard of the subpoena power under the SCA gives the government blanket permission to search *any* data that it has a reasonable belief to be relevant to an ongoing criminal investigation.[219] For example, the government may have "reasonable grounds to believe" that data on the smart home device has a piece of information that will lead to evidence of a crime. However, the government might not know exactly what day or time that data will be found. Under the SCA, the government may be able to find not only evidence related to the criminal investigation, but also information regarding *every* other aspect of that user's life within their home.[220] The SCA gives arbitrary governmental power, basically allowing it to do whatever it wants with the data collected, and thereby running afoul of any Fourth Amendment protections. Therefore, because of the nature and amount of information that the government would have access to under the SCA, particularity of a search warrant must be

---

[212] Camara v. S.F. Mun. Ct., 387 U.S. 523, 528 (1967).
[213] Smith v. Maryland, 442 U.S. 735, 740 (1979) (internal quotes and brackets omitted).
[214] *See* 18 U.S.C. § 2703(d); *Carpenter*, 138 S. Ct. at 2221.
[215] Groh v. Ramirez, 540 U.S. 551, 557 (2004).
[216] *See id.*
[217] *Id.*
[218] *See* 18 U.S.C. § 2703(d).
[219] *Id.*
[220] *See id.*; *supra* note 191.

https://ecommons.udayton.edu/udlr/vol45/iss1/7

required to gain access to smart home devices.

The dissent in *Carpenter* suggested that by requiring a search warrant for CSLI data, criminal investigations would be put at serious risk and place undue restrictions on law enforcement.[221] However, this would not be the case for smart home devices. Requiring a warrant would ensure that police are obtaining particularized, specific information actually relevant to a criminal investigation, rather than getting unlimited access to the user's data once the lesser "reasonable grounds" standard is met.[222] By requiring a search warrant, law enforcement, and the government in general, is held accountable for their actions and the requirements of the Fourth Amendment.[223]

IV. CONCLUSION

As technology continues to grow and become more advanced, the Court must seek to ensure that individuals have adequate protection against governmental intrusion. Because of the ample amount of personal information contained on smart home devices, a court order issued under the SCA does not protect a user's reasonable expectation of privacy. In *Carpenter*, the Supreme Court addressed the ability of the government to encroach on private areas of one's life and held that the SCA does not provide adequate protection to CSLI data.[224] Based on the decision in *Carpenter*, the SCA also does not provide adequate privacy protection to information stored on smart home devices.[225]

Smart home devices provide a chronicle of one's personal life, thus allowing the government to track movements, activities, attitudes, hobbies, and even content of private conversations.[226] Because of the type of information that could be gathered from smart home devices, the traditional third-party doctrine cannot be extended to include these devices.[227] Under the SCA, the standard for obtaining data from smart home devices would be "reasonable grounds to believe that the contents . . . are relevant and material to an ongoing investigation."[228] The standard under the SCA is simply not strict enough to protect one's private life considering, the sensitive type of information on smart home devices. Therefore, a warrant supported by probable cause must be issued in order for the government to obtain this data,

---

[221] *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (Kennedy, J., dissenting).

[222] *See id.* at 2222–23.

[223] Barry Friedman and Orin Kerr, *The Fourth Amendment*, NAT'L CONST. CTR., https://constitutioncenter.org/interactive-constitution/interpretation/amendment-iv/interps/121; *see also* U.S. CONST. amend. IV; United States v. Hanon, 428 F.2d 101, 104 (8th Cir. 1970).

[224] *See Carpenter*, 138 S. Ct. at 2221.

[225] *See id.* at 2223.

[226] *How Google and Amazon Are 'Spying' on You*, CONSUMER WATCHDOG, https://www.consumerwatchdog.org/privacy-technology/how-google-and-amazon-are-spying-you (last visited Feb. 15, 2020).

[227] *See supra* Section III.D.

[228] 18 U.S.C. § 2703(d) (2012).

Published by eCommons, 2020

listing the particularities of what is to be gathered.[229] Requiring a warrant would keep the government accountable by ensuring that police are obtaining specific information that is actually relevant to the ongoing investigation, rather than just having a "reasonable suspicion" that data on the smart home device relates to the crime.[230] Without this requirement, law enforcement could always create some reason justifying that they think there is relevant data on a smart home device. The SCA creates expectations of privacy that are ultimately illusory and meaningless.[231] Without requiring a warrant under the Fourth Amendment, there is essentially no way that users of smart home devices have enough protection against the government from obtaining their personal data.[232]

Throughout the United States, and the world in general, the state of technology continues to advance.[233] The law cannot keep up with the pace of change in technology.[234] The Internet's capabilities are expanding rapidly with smart home devices.[235] Precautionary measures must be taken in order to protect the data stored on these devices. When more technology arises, too much government encroachment into one's private affairs may also arise. Although the Supreme Court has not addressed the issue of smart home devices and the government's ability to search and seize the personal data from them, precautions should to be taken before the government significantly intrudes on one's private affairs.

The Internet's capacity continues to expand rapidly with the addition of new technologies, including smart home devices. "The viability of . . . technology and its growing acceptance by consumers and service providers offer[s] powerful evidence that a lasting technological and societal shift is underway."[236] As a result of this change and growth in technology, courts need to determine whether existing laws provide adequate protection from governmental intrusion. People seek to preserve activities within their homes as private, and because smart home devices record a person's activities within their home, a warrant supported by probable cause must be required in order to obtain data from these devices.[237]

---

[229] *See* Friedman & Kerr, *supra* note 222.

[230] *Id.*

[231] Robison, *supra* note 73, at 1196.

[232] *See supra* Section III.D.

[233] *See generally* Bill Gates et al., *How We'll Invent the Future, By Bill Gates*, MIT TECH. REV. (Feb. 27, 2019), https://www.technologyreview.com/lists/technologies/2019/.

[234] Julia Griffith, *A Losing Game: The Law is Struggling to Keep up with Technology*, JHTL (Apr. 12, 2019), https://sites.suffolk.edu/jhtl/2019/04/12/a-losing-game-the-law-is-struggling-to-keep-up-with-technology/.

[235] *See* Hannah Bouckley, *6 Easy Steps to Turn Your House Into a Smart Home*, BRITISH TELECOMM. (July 19, 2019), https://home.bt.com/tech-gadgets/internet/connected-home/the-connected-home-or-smart-home-explained-what-does-it-mean-11363866334872.

[236] Robison, *supra* note 73, at 1204.

[237] *See supra* Section III.D.

https://ecommons.udayton.edu/udlr/vol45/iss1/7

Though technology of smart home devices has given law enforcement a powerful new tool for carrying out its responsibilities, it has also given law enforcement a powerful tool for obtaining private information about one's life, simply by using the "reasonable grounds" standard under the SCA.[238] The SCA requirement falls well short of the probable cause standard required for a warrant.[239] Technology has become such a normal part of daily life, and because of this, the progress of science cannot erode Fourth Amendment protections.[240] Therefore, a search warrant should be required in order for the government to obtain data from smart home devices.

[238] *Id.*

[239] *See supra* Section II.C.; 18 U.S.C. § 2703(d) (2012); Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018); *see also supra* note 25.

[240] Olmstead v. United States, 277 U.S. 438, 474 (1928).

Published by eCommons, 2020