Boston College Law Review

Volume 61 | Issue 2 Article 9

2-27-2020

Watt Now?: Smart Meter Data Post-*Carpenter*

Sarah Murphy
Boston College Law School, sarah.murphy.8@bc.edu

WATT NOW?: SMART METER DATA POST-*CARPENTER*

Abstract: Smart meters, which automatically relay energy consumption data to utility companies, are increasingly displacing traditional energy meters. Data collected from smart meters has elicited widespread concern because it can reveal considerable information about what goes on inside a home. For example, smart meter data can uncover when a person is home, away, or asleep. Historically, utility records have not been afforded Fourth Amendment protection due to the third-party doctrine: a person forfeits Fourth Amendment rights when information is voluntarily conveyed to third parties. In 2018, however, the Supreme Court in *Carpenter v. United States* recognized an individual's Fourth Amendment rights in data held by a third party. In doing so, *Carpenter* held that a warrant is required in the "rare case" where a person has Fourth Amendment rights in data held by a private third party. Additionally, in 2018, the Seventh Circuit held in *Naperville Smart Meter Awareness v. City of Naperville* that individuals have Fourth Amendment rights in the collection of their smart meter data in certain circumstances. *Naperville* did not address law enforcement access to smart meter data. This Note explains why smart meter data deserves Fourth Amendment protection and posits that smart meter data should fit squarely within the "rare case" envisioned by the Supreme Court in *Carpenter*. As such, this Note argues that a warrant supported by probable cause be required for law enforcement to access smart meter data.

INTRODUCTION

In the United States, there has long been concern about the level of government encroachment into the private affairs of citizens.[1] In the context of the

[1] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195, 220 (1890) (tracing the development of legal remedies enacted to protect a person's right "to be let alone" and noting that the common law has historically treated "a man's house as his castle"). *The Right to Privacy*, a famous article written in 1890 by Samuel D. Warren and Louis Brandeis, gave rise to state recognition of privacy torts. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 39 (2017); *see* James H. Barron, *Warren and Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890): Demystifying a Landmark Citation*, 13 SUFFOLK U. L. REV. 875, 877 (1979) (attributing the tort of invasion of privacy to Warren and Brandeis); Benjamin E. Bratman, *Brandeis and Warren's* The Right to Privacy *and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623, 624 (2002) (describing the article as "legendary" and the driving force behind a "right to privacy" in the United States); Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CATH. U.L. REV. 703, 704 (1990) (noting that Warren and Brandeis "gave birth" to privacy law). Warren and Brandeis feared tabloids and what might result from technological developments, such as instant photography and audio recordings. *See* Warren & Brandeis, *supra*, at 195 (arguing that technological advancements "threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'"). Today, we are living in an age where 'Alexa' and 'Siri' are so

home, the Fourth Amendment to the U.S. Constitution protects "[t]he right of the people to be secure in their persons, *houses*, papers, and effects against unreasonable searches and seizures."[2] The concept of a home being an individual's "castle and fortress" can be traced back to the ingenuity of English judge Sir Edward Coke.[3] Moreover, the infamous "writs of assistance" that allowed British officers to enter any home without notice, was one of the factors that led to the American Revolution.[4]

Recently, smart meters have raised concerns about privacy in the home.[5] More troublesome than a nosy neighbor, smart meters have the potential to track and record what a person does in the home to a high degree of accuracy.[6] Smart meters are the result of modernized traditional gas and energy meters.[7]

---

commonplace that people can confuse their "servant robots." Pepto Abysmal (@roastedryebread), TWITTER (Jan. 9, 2019, 10:19 AM), https://twitter.com/roastedryebread/status/1083065853518655489 [https://perma.cc/6Y9W-GQB7]. Alexa is a device engineered by Amazon, which acts as a "virtual assistant," designed to be used in a person's home. Kim Wetzel, *What Is Alexa, and What Can Amazon's Virtual Assistant Do for You?*, DIGITAL TRENDS (Feb. 16, 2019), https://www.digitaltrends.com/home/what-is-amazons-alexa-and-what-can-it-do/ [https://perma.cc/R2YW-U95S]. Alexa can help perform various tasks such as playing music, turning on lights, and looking up information online. *Id.* Siri, an Apple service, performs similar functions. *See* APPLE, https://www.apple.com/siri/ [https://perma.cc/75MF-P7QH] (noting that Siri can set alarms, find directions, play music, unlock doors, and turn on lights).

[2] U.S. CONST. amend. IV (emphasis added).

[3] *See* Semayne's Case, 77 Eng. Rep. 194, 194–95 (K.B. 1604) (noting that "the house of every one is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose").

[4] Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 301 (1967).

[5] *See* Cheryl D. Balough, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161, 161, 190–91 (2011) (discussing some of the privacy concerns associated with smart meters and advocating for a federal legislative action to safeguard individual privacy); Natasha Duarte, *The Home Out of Context: The Post-*Riley *Fourth Amendment and Law Enforcement Collection of Smart Meter Data*, 93 N.C. L .REV. 1140, 1144 (2015) (explaining that smart meter data can be analyzed to reveal private information); Megan McLean, *How Smart Is Too Smart?: How Privacy Concerns Threaten Modern Energy Infrastructure*, 18 VAND. J. ENT. & TECH. L. 879, 885 (2016) (recognizing that smart meters can reveal personal details about what a person does in their home and can be valuable to law enforcement).

[6] *See* CONG. RES. SERV., SMART METER DATA: PRIVACY AND CYBERSECURITY 3–4 (2012) [hereinafter CRS SMART METER REPORT] (noting that smart meters provide granular information about energy data consumption by measuring data consumption every fifteen minutes); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (demonstrating that cell phone carriers are not like typical witnesses: "unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible"). In the case of smart meter data, if a nosy neighbor watches your home to see when the lights go on and off, he or she might be able to infer your daily routine—when you wake up in the morning, when you go to sleep, when you are home, and when you leave. *See id.* (distinguishing a cell phone carrier from a nosy neighbor). Unlike a nosy neighbor, however, a smart meter is always present and collecting precise data to a high degree of certainty. *See id.* (noting that there is a difference between what information a neighbor could gather and what information a cell phone carrier can gather); CRS SMART METER REPORT, *supra*, at 4 (describing the detailed nature of frequent smart meter data collection).

[7] NAT'L INST. STANDARDS & TECH., GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 2 (2014) [hereinafter NIST SMART GRID REPORT].

Traditional meters require an employee to manually check and report how much electricity is used each month.[8] In contrast, smart meters can wirelessly send data to utility companies every fifteen minutes.[9] As a result, compared to the one lump sum number collected in a traditional meter each month, smart meter data is more precise because the data is collected every fifteen minutes.[10] Because of this frequent data collection, smart meter data can reveal what appliances are present in a home and when they are in use.[11] By tracking a person's interactions with home appliances, smart meter data can uncover, for example, when a person is home, away, or asleep.[12] These types of inferences can be extremely threatening to the privacy that a person expects to have in her home, a place traditionally deserving of the highest privacy protections.[13]

---

[8] *Id.*

[9] CRS SMART METER REPORT, *supra* note 6, at 3–4. A smart meter is part of an Advanced Metering Infrastructure (AMI). *Id.* at 1. AMI refers to the complete measuring, collection, and communication system between the customer and a utility provider. U.S. DEP'T OF ENERGY, ADVANCED METERING INFRASTRUCTURE AND CUSTOMER SYSTEM: RESULTS FROM THE SMART GRID INVESTMENT GRANT PROGRAM 4 (2016) [hereinafter U.S. DEP'T OF ENERGY, AMI REPORT].

[10] CRS SMART METER REPORT, *supra* note 6, at 3–4; *see also* NIST SMART GRID REPORT, *supra* note 7, at 9 (finding that most smart meters collect data either once every hour or once every fifteen minutes).

[11] CRS SMART METER REPORT, *supra* note 6, at 4. This is because each appliance has a unique electric load signature which corresponds to energy usage. *Id.* For example, a television uses power differently than a refrigerator. Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 524 (7th Cir. 2018).

[12] U.S. DEP'T OF ENERGY, DATA ACCESS AND PRIVACY ISSUES RELATED TO SMART GRID TECHNOLOGIES 2 (2010) [hereinafter U.S. DEP'T OF ENERGY, SMART GRID REPORT]. Smart meters can discern:

> Whether individuals tend to cook microwavable meals or meals on the stove; whether they have breakfast; the time at which individuals are at home; whether a house has an alarm system and how often it is activated; when occupants usually shower; when the TV and/or computer is on; whether appliances are in good condition; the number of gadgets in the home; if the home has a washer and dryer and how often they are used; whether lights and appliances are used at odd hours, such as in the middle of the night; whether and how often exercise equipment such as a treadmill is used.

INFORMATION & PRIVACY COMMISSIONER OF ONTARIO & THE FUTURE OF PRIVACY FORUM, SMART PRIVACY FOR THE SMART GRID: EMBEDDING PRIVACY INTO THE DESIGN OF ELECTRICITY CONSERVATION 11 (2009) [hereinafter SMARTPRIVACY FOR THE SMART GRID]. In addition, smart meters can provide the inference that a person is "sleep deprived," infrequently does laundry, or is typically away from the home until bars close. *Id.*; *see* Rouzbeh Razavi, *Rethinking the Privacy of the Smart Grid: What Your Smart Meter Data Can Reveal About Your Household in Ireland*, 44 ENERGY RES. & SOC. SCI. 312, 312–23 (2018) (using various algorithms to accurately predict household size).

[13] *See* Florida v. Jardines, 569 U.S. 1, 6 (2013) (emphasizing that the home is "first among equals" in the eyes of the Fourth Amendment); California v. Ciraolo, 476 U.S. 207, 213 (1986) (finding that "privacy expectations are most heightened" in the context of the home); Oliver v. United States, 466 U.S. 170, 180 (1984) (reaffirming the notion that the Fourth Amendment applies to areas "immediately surrounding and associated with the home"); Silverman v. United States, 365 U.S. 505, 511 (1961) (noting that "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"); Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV.

Smart meter data could be invaluable in criminal investigations.[14] Courts have concluded that law enforcement access to similar utility records is not a "search" under the Fourth Amendment due to the third-party doctrine—the principle that the Fourth Amendment does not protect information that is voluntarily disclosed to a third party.[15] In 2018, however, the Supreme Court in *Carpenter v. United States* limited the application of the third-party doctrine by refusing to apply it to records containing cell-site location information.[16] Instead, the Court held that when a person has a significant privacy interest in records stored with a third party—a "rare case"—a search requires a warrant.[17] In doing so, *Carpenter* effectively limited the blanket application of the third-party doctrine and required a case-by-case evaluation to determine a person's

905, 912–13 (2010) (referring to the home as a "sacred site" in Supreme Court Fourth Amendment jurisprudence and describing the Fourth Amendment protections of the home as an "enshrinement," reaching an "iconic status").

[14] Duarte, *supra* note 5, at 1140–41; *see* Daniel Zwerdling, *Your Home Is Your . . . Snitch?*, MARSHALL PROJECT (May 24, 2018), https://www.themarshallproject.org/2018/05/24/your-home-is-your-snitch, [https://perma.cc/W5YN-8R7K] (discussing how smart appliances could aid law enforcement in monitoring individuals). For example, law enforcement could use the data to determine whether a home contains a marijuana grow light or whether someone was home when she claimed to be. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2212 (involving a situation where law enforcement sought to identify a person's location at specific moments in time to determine whether it was feasible for that person to have committed a crime); Kyllo v. United States, 533 U.S. 27, 29 (2001) (describing a law enforcement agent's use of a high energy meter reading to confirm the fact that a person was growing marijuana in his home). A person's habits in the home can also be important for determining whether a person has the authority to consent to a Fourth Amendment search of the home. *See, e.g.*, United States v. Corral, 339 F. Supp. 2d 781, 792 (W.D. Tex. 2004) (explaining that a housekeeper could not consent to a search of the defendant's home because she only cleaned the house a couple of times per week); State v. Shumaker, 914 So. 2d 1156, 1167 (La. Ct. App. 2005) (holding that a babysitter had the authority to consent to search common areas of the home and the trailer in the yard because she often stayed overnight at the residence).

[15] *See* U.S. CONST. amend. IV (prohibiting "unreasonable searches and seizures"); United States v. McIntyre, 646 F.3d 1107, 1111–12 (8th Cir. 2011) (holding that the Fourth Amendment did not apply because power records were voluntarily conveyed to the utility company); United States v. Porco, 842 F. Supp. 1393, 1398 (D. Wyo. 1994) (denying Fourth Amendment protection to energy records); *see also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that the Fourth Amendment did not apply when the defendant dialed numbers on his phone because he voluntarily communicated that information to the phone company for a business purpose); United States v. Miller, 425 U.S. 435, 440 (1976) (finding that business records of banks are not like "private papers" typically entitled to Fourth Amendment protection). The third-party doctrine has been a source of legal controversy. *Compare* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (defending the third-party doctrine) [hereinafter Kerr, *Case for the Third-Party Doctrine*] *with* Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211 (2006) (arguing that *Smith*, *Miller*, and other third-party doctrine cases were wrongly decided). *See Carpenter*, 138 S. Ct. at 2261–72 (Gorsuch, J., dissenting) (criticizing the third-party doctrine).

[16] *Carpenter*, 138 S. Ct. at 2223.

[17] *Id.* at 2222.

privacy interest in records held by a third party.[18] As a result, *Carpenter* opened the door for courts to consider the applicability of the Fourth Amendment to smart meter data.[19]

In fact, in 2018, the U.S. Court of Appeals for the Seventh Circuit relied on *Carpenter* in holding that a public utility's collection of smart meter data is a reasonable search under the Fourth Amendment.[20] Although the Seventh Circuit did not address law enforcement collection of smart meter data,[21] officers are likely to request such data in the near future due to the helpful inferences that the data can provide.[22]

---

[18] *See id.* at 2222–23 (holding that a person has a reasonable expectation of privacy in cell-site location information data).

[19] *See* Balough, *supra* note 5, at 183–85 (finding that pre-*Carpenter* case law might not be sufficient to find that the Fourth Amendment applies to smart meter data); Mihailis E. Diamantis, *Privileging Privacy: Confidentiality as a Source of Fourth Amendment Protection*, 21 U. PA. J. CONST. L. 486, 488–90 (2018) (discussing *Carpenter*'s re-shaping of the third-party doctrine); Duarte, *supra* note 5, at 1164 (positing that the Fourth Amendment fails to protect smart meter data due to the third-party doctrine); Jessica Lile, Comment, *Internet Privacy Regulations and the* Carpenter *Decision*, 87 UMKC L. REV. 777, 799 (2019) (arguing that *Carpenter*'s holding allows for a Fourth Amendment application to data sought from Internet Service Providers); McLean, *supra* note 5, at 894 (contending that smart meter data is not protected by the Fourth Amendment due to the third-party doctrine and the "general public use" exception); Nameir Abbas et al., Carpenter *Ruling May Be Turning Point in Digital Data Privacy*, LAW360 (Aug. 8, 2018), https://www.law360.com/articles/1069397/carpenter-ruling-may-be-turning-point-in-digital-data-privacy [https://perma.cc/VN8U-37CV] (examining *Carpenter*'s cutting back of the third-party doctrine). *See generally* CRS SMART METER REPORT, *supra* note 6, at 6–22 (discussing the Fourth Amendment's applicability to smart meter data pre-*Carpenter*).

[20] *Naperville*, 900 F.3d at 527, 529.

[21] *Id. Naperville* was a civil case involving a public utility that installed smart meters without the consent of Naperville citizens. *Id.*

[22] NIST SMART GRID REPORT, *supra* note 7, at 11; *see* Eoghan McKenna et al., *Smart Meter Data: Balancing Consumer Privacy Concerns with Legitimate Applications*, 41 ENERGY POL'Y 807, 808 (2012) (summarizing privacy concerns associated with smart meters). Amazon's "Alexa" exemplifies some of the privacy concerns resulting from new technology. Niraj Chokshi, *Is Alexa Listening? Amazon Echo Sent Out Recording of Couple's Conversation*, N.Y. TIMES (May 25, 2018), https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html [https://perma.cc/EN96-9HJR]. This is because of Alexa's ability to listen and record audio when inactive. *Id.* Specifically, Alexa activates when the wake word "Alexa" is spoken. *Id.* To hear the wake word, however, Alexa must always be listening. *Id.* Moreover, Alexa records audio a few seconds before and after the wake word is spoken. *Id.* If the user does not delete this data, Amazon keeps these records indefinitely. Sharon Profis & Rick Broida, *Amazon Echo Saves All Your Voice Data. Here's How to Delete It.*, CNET (May 31, 2018), https://www.cnet.com/how-to/amazon-echo-saves-all-your-voice-data-heres-how-to-delete-them/ [https://perma.cc/MK54-PAAS]. Recently, law enforcement has requested data from Amazon's "Alexa" to help aid in murder investigations. *See, e.g.*, Cyrus Farivar, *Alexa: What Did You Hear?—Amazon Must Give Up Echo Recordings in Double Murder Case, Judge Rules*, ARS TECHNICA (Nov. 10, 2018), https://arstechnica.com/tech-policy/2018/11/amazon-must-give-up-echo-recordings-in-double-murder-case-judge-rules/ [https://perma.cc/JDL4-AAW9] (discussing the seizing of Alexa audio data, and information about whose phone was connected to the Alexa in connection with a January 2017 New Hampshire murder case where two women were murdered in a kitchen that contained an Alexa device); Elliot C. McLaughlin, *Suspect OKs Amazon to Hand Over Echo Recordings in Murder Case*, CNN (Apr. 26, 2017), https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html [https://perma.cc/XY5L-

Part I of this Note develops the Fourth Amendment framework for searches of the home and provides a history of the third-party doctrine.[23] Part I also explains the legal standards involved when law enforcement obtains a subpoena and a warrant.[24] Part II summarizes *Carpenter*'s recognition of an individual's Fourth Amendment rights in remotely stored information.[25] Part III provides an overview of smart meter data and discusses the Seventh Circuit case that recognizes the privacy interests in smart meter data.[26] Part IV explains why the collection of smart meter data implicates the Fourth Amendment.[27] Part IV also argues that law enforcement should be allowed to access smart meter data, whether held by a public or private utility company, only after first obtaining a warrant.[28]

I. THE FOURTH AMENDMENT'S APPLICABILITY TO SMART METER DATA

Access to smart meter data by law enforcement raises significant privacy concerns.[29] For example, how does society grapple with Fourth Amendment protections at a time when technology is rapidly advancing?[30] There is a deli-

---

W6QM] (describing a 2017 Arkansas murder case and noting that Alexa audio recordings were sought when a witness noted that Alexa was streaming music during the night in question). In the 2017 Arkansas murder case, prosecutors sought data from the suspect's smart water heater because it showed that the suspect used an abnormally large amount of water early in the morning, indicating an attempt to clean up the murder. *Id.* Similarly, prosecutors sought Siri data in connection with a 2012 Florida murder, during which a man asked Siri where he could hide a dead body and then proceeded to use his flashlight application on his phone nine times. Yoni Heisler, *Murder Suspect Asks Siri Where to Hide a Dead Body*, NETWORK WORLD (Aug. 13, 2014), https://www.networkworld.com/article/2464546/murder-suspect-asks-siri-where-to-hide-a-dead-body.html [https://perma.cc/D9FC-XS9L].

[23] *See infra* notes 29–96 and accompanying text.

[24] *See infra* notes 97–139 and accompanying text.

[25] *See infra* notes 140–185 and accompanying text.

[26] *See infra* notes 186–247 and accompanying text.

[27] *See infra* notes 248–288 and accompanying text.

[28] *See infra* notes 289–320 and accompanying text.

[29] CRS SMART METER REPORT, *supra* note 6, at 5; NIST SMART GRID REPORT, *supra* note 7, at 11; U.S. DEP'T OF ENERGY, AMI REPORT, *supra* note 9, at 4; U.S. DEP'T OF ENERGY, SMART GRID REPORT, *supra* note 12, at 49; Balough, *supra* note 5, at 191; Duarte, *supra* note 5, at 1140–41; McLean, *supra* note 5, at 885.

[30] *See* Balough, *supra* note 5, at 171–72 (noting that smart meter data could greatly benefit law enforcement agencies and discussing some of the privacy concerns arising therefrom); Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004) (discussing an evolving Fourth Amendment framework in response to new technologies) [hereinafter Kerr, *The Fourth Amendment and New Technologies*]. Notwithstanding its benefits to society, technology has raised serious privacy concerns. *See* Nils Backe, *Is Amazon Alexa Invading Privacy? Analysis of an Ethical Dilemma*, MEDIUM (Nov. 26, 2018), https://medium.com/@nils.backe/is-amazon-alexa-invading-privacy-analysis-of-an-ethical-dilemma-f7e064ab6dba [https://perma.cc/TX5Q-LJ69] (discussing several consumer privacy issues involved in Alexa data but concluding that Amazon is acting ethically and responsibly given its role as a leader in the technology space); Eli Blumenthal, *Facebook's Latest Privacy Scandal: What We Know About the Company's Handling of User Data*, USA TODAY (Dec. 19, 2018), https://www.usatoday.com/story/tech/2018/12/19/facebooks-latest-privacy-scandal-what-we-know-now/2361257002/ [https://perma.cc/F4VF-

cate balance between protecting Fourth Amendment rights and enabling law enforcement to investigate crimes effectively.[31] As a result, the Supreme Court has recognized the need for a flexible approach to the Fourth Amendment to protect against encroachment into private spheres in the digital age.[32]

This Part explores the current Fourth Amendment framework as applied to searches of the home, particularly in the context of utility data.[33] Section A of this Part provides a summary of the Fourth Amendment framework and highlights three areas of the Fourth Amendment that may apply to smart meter data.[34] Section B explores several different mechanisms by which the government may compel the production of records and the different legal standards for each. [35] Section B then examines how law enforcement agencies use subpoenas to access traditional energy data and smart meter data.[36]

A. Fourth Amendment Framework

To trigger the Fourth Amendment, there are two requirements.[37] First, there must be government action.[38] Second, the government action must be

---

TFBG] (explaining various privacy scandals involving Facebook, including the Facebook Cambridge Analytica scandal, arising after Facebook collected personal information of users and sold it to third parties); Bennett Cyphers, *Data Privacy Scandals and Public Policy Picking Up Speed: 2018 in Review*, ELECTRONIC FRONTIER FOUND. (Dec. 31, 2018), https://www.eff.org/deeplinks/2018/12/data-privacy-scandals-and-public-policy-picking-speed-2018-year-review [https://perma.cc/P7NH-ZKPV] (describing major privacy scandals of technology companies, such as Facebook and Google); Julia Pagnamenta, *Can Alexa Testify Against You?*, CRIME REP. (Mar. 22, 2018), https://thecrimereport.org/2018/03/22/alexa-get-me-the-first-amendment/ [https://perma.cc/3JNN-TJ77] (explaining the privacy implications of Alexa data and the applicability of the First Amendment and Fourth Amendment to Alexa data). *See generally* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004) (shedding light on how technology allows for a greater free flow of personal information, which can pose a large threat to privacy). In response to these privacy concerns, legislatures have begun to tackle privacy issues more seriously. Cyphers, *supra*.

[31] *See* ROBERT M. BLOOM, SEARCHES, SEIZURES, AND WARRANTS 46 (2003) (arguing that society is worse off if police are heavily restricted because it makes it harder to investigate crimes).

[32] *See Carpenter*, 138 S. Ct. at 2214 (noting that "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted'" (quoting *Kyllo*, 533 U.S. at 34)); *Kyllo*, 533 U.S. at 28 (rejecting a "mechanical interpretation" of the Fourth Amendment).

[33] *See infra* notes 29–185 and accompanying text.

[34] *See infra* notes 37–96 and accompanying text.

[35] *See infra* notes 97–120 and accompanying text.

[36] *See infra* notes 121–139 and accompanying text.

[37] ROBERT M. BLOOM & MARK S. BRODIN, CRIMINAL PROCEDURE: THE CONSTITUTION AND THE POLICE 17 (8th ed. 2016). The Fourth Amendment protects "persons, houses, papers, and effects." U.S. CONST. amend. IV.

[38] *See* Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (holding that an illegal search conducted by private persons did not implicate the Fourth Amendment). This Note assumes that there has already been some level of state action that has triggered the Fourth Amendment. *Compare* People v. Perlos, 462 N.W.2d 310, 314 (Mich. 1990) (holding that the Fourth Amendment did not apply to a blood draw because there was no state action), *with* Jones v. Murray, 962 F.2d 302, 306 (4th Cir.

considered a "search" or a "seizure."[39] If these requirements are met, the Fourth Amendment applies and a court must determine whether the search was reasonable.[40] In 1967, in *Katz v. United States*, the Supreme Court abandoned a strict application of the Fourth Amendment in favor of a flexible one.[41] Justice Harlan's concurrence later became the *Katz* test, or the "reasonable expectation of privacy" test, recognizing that a Fourth Amendment search could occur without physical entry.[42] To determine whether the Fourth Amendment applies, the *Katz* test asks two questions: (1) whether there is a subjective reasonable expectation of privacy; and (2) if there is, whether that expectation is one that society would recognize as reasonable.[43]

Three different categories of cases are relevant when considering the Fourth Amendment implications on the collection of smart meter data by law enforcement.[44] One category discusses the reasonable expectations of privacy that individuals have in the home.[45] Another considers what expectations of

---

1992) (explaining that the Fourth Amendment applied to a state statute that required felons to submit blood samples). It is important to emphasize that *Naperville* involved non-criminal, non-investigatory conduct. *Naperville*, 900 F.3d at 529. In that case, the court found "state action" simply because the public utility collecting the data was owned by the state. *Id.* at 528. The public utility existed to perform traditional utility company tasks and did not aim to "spy" on its residents by installing smart meters in every citizen's home in Naperville. *See id.* (explaining that Naperville did not install smart meters with "prosecutorial intent").

[39] Katz v. United States, 389 U.S. 347, 353 (1967).

[40] *See* United States v. Knights, 534 U.S. 112, 118 (2001) (emphasizing that "the touchstone of the Fourth Amendment is reasonableness").

[41] *Katz*, 389 U.S. at 353 (holding that the Federal Bureau of Investigation's (FBI) placing of a recording device on a phone booth to record a suspect's conversations was an unconstitutional search); *see* U.S. CONST. amend. IV (protecting "persons, houses, papers, and effects"). Historically, the Fourth Amendment applied only to those areas enumerated in the amendment. U.S. CONST. amend. IV. Prior to 1967, a Fourth Amendment "search" took place when there was a common law trespass. *See, e.g.*, Goldman v. United States, 316 U.S. 129, 134 (1942) (examining whether a search was made via illegal trespass); Olmstead v. United States, 277 U.S. 438, 464–66, (1928), *overruled by Katz*, 389 U.S. at 347, *and* Berger v. New York, 388 U.S. 41, 41 (1967) (holding that the Fourth Amendment was not violated when a government agent wiretapped a phone because there was no trespass).

[42] *Katz*, 389 U.S. at 360 (Harlan, J., concurring). This test has been widely criticized. *See generally* Kevin Emas & Tamara Pallas, United States v. Jones*: Does* Katz *Still Have Nine Lives?*, 24 ST. THOMAS L. REV. 116 (2012); Orin Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113 (2015); Daniel T. Pesciotta, *I'm Not Dead Yet:* Katz, Jones, *and the Fourth Amendment in the 21st Century*, 63 CASE W. RES. 187 (2012); Matthew Tokson, *Blank Slates*, 59 B.C. L. REV. 591 (2018).

[43] *Katz*, 389 U.S. at 360 (Harlan, J., concurring); *see, e.g.*, United States v. Diaz-Castaneda, 494 F.3d 1146, 1153 (9th Cir. 2007) (holding that license plate numbers are not protected by the Fourth Amendment because a person's subjective expectation of privacy in a license plate number is not one society would recognize as reasonable).

[44] *See Carpenter*, 138 S. Ct. at 2215–16 (analyzing the Fourth Amendment claim by looking at the applicable cases in two categories).

[45] *See infra* notes 49–61 and accompanying text.

privacy individuals have in information turned over to third parties.[46] The final category is a new area represented by *Carpenter* and other similarly situated cases that do not fit neatly into the existing Fourth Amendment framework.[47] Each of these categories is examined below.[48]

1. Expectation of Privacy in the Home

The Supreme Court has consistently placed a high value on privacy inside the home and in areas surrounding the home.[49] In 2001, the Supreme Court, in *Kyllo v. United States*, held that the collection of thermal images of a person's home by law enforcement, taken from outside of the home, was a search.[50] There, a federal agent suspected that Danny Kyllo was growing marijuana.[51] To investigate his suspicions, the agent used a thermal imaging device to scan Kyllo's home.[52] The scan revealed that parts of the home emanated an abnormal amount of heat, consistent with halide heat lamps typically used to grow marijuana.[53]

Recognizing that the agent engaged in a "more than naked-eye surveillance of a home," the Court emphasized that the thermal imaging device allowed law enforcement to obtain information it otherwise would not have been able to access without physical entry.[54] Holding that the scan was a warrantless

---

[46] *See infra* notes 62–73 and accompanying text.

[47] *See infra* notes 74–96 and accompanying text.

[48] *See infra* notes 49–96 and accompanying text.

[49] BLOOM & BRODIN, *supra* note 37, at 27; *see Jardines*, 569 U.S. at 6 (recognizing the home as the "first among equals" and holding that the Fourth Amendment applied to a dog sniff of a home); *Silverman*, 365 U.S. at 511 (emphasizing that "[a]t the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion"); Boyd v. United States, 116 U.S. 616, 630 (1886) (noting that the Fourth Amendment protects the "sanctity of a man's home"). Additionally, courts have protected the area immediately surrounding the home, referred to as the "curtilage." *See, e.g.*, Collins v. Virginia, 138 S. Ct. 1663, 1670 (2018) (finding that a driveway was "curtilage" of the home and the Fourth Amendment's protections of curtilage has "long been black letter law"); *Ciraolo*, 476 U.S. at 212–13 (noting that the Fourth Amendment's protection of the "curtilage" is "essentially a protection of families and personal privacy in an area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened"); *see also* Hester v. United States, 265 U.S. 57, 58–59 (1924) (holding that law enforcement can gather information in "open fields" because such fields are not enumerated in the Fourth Amendment).

[50] *Kyllo*, 533 U.S. at 40. Additionally, officers subpoenaed the utility company and determined that he had increased electricity usage. *Id.* at 44 (Stevens, J., dissenting).

[51] *Id.* at 29 (majority opinion).

[52] *Id.* Thermal imaging devices detect infrared radiation and convert the radiation into an image. *Id. See generally* U.S. DEP'T OF HOMELAND SECURITY, SYSTEM ASSESSMENT AND VALIDATION FOR EMERGENCY RESPONDERS: HAND-HELD THERMAL IMAGING DEVICES (2007) (describing the science behind thermal imaging devices). The image is created based on a correlation of warmth to color, where black corresponds to cold and white corresponds to hot. *Kyllo*, 533 U.S. at 29–30.

[53] *Kyllo*, 533 U.S. at 30. Specifically, the scan revealed that the garage roof and a side wall were exceptionally warm compared to the rest of the home. *Id.* Moreover, the scan showed that these parts of Kyllo's home were significantly hotter than other homes in the area. *Id.*

[54] *Id.* at 33, 40.

search, the Court found it significant that the thermal imaging device was not "in general public use."[55] Moreover, the Court recognized that an inference can give rise to a Fourth Amendment violation.[56] Although the thermal device merely showed images, the images led to the inference that Kyllo was growing marijuana.[57] Ultimately, the Supreme Court pronounced that, absent a warrant, the government could not capitalize on technology to explore what was going on inside a home because it would leave homeowners "at the mercy of advancing technology."[58]

In addition to the line of cases recognizing the expectation of privacy in the home, there may also be an expectation of privacy in information given to third parties.[59] This is relevant for smart meter data because the data is typically sent to a third-party utility company.[60]

2. Expectation of Privacy in Information Voluntarily Turned Over to Third Parties

The third-party doctrine is an exception to the *Katz* test.[61] It is the notion that a person does not have a reasonable expectation of privacy in information voluntarily provided to third parties.[62] Between 1952 and 1971, the Supreme Court created and developed the third-party doctrine in the context of "secret agents," or undercover police officers.[63] In those cases, the Court held that a

---

[55] *Id.* at 34. The dissent criticized the majority's interjection of the "general public use" standard because it allows Fourth Amendment protections to disappear merely when the relevant technology is popular. *Id.* at 46–47 (Stevens, J., dissenting). Moreover, the dissent highlighted the imprecise nature of general public use, noting that it is difficult to determine how prevalent the technology must be to brand it in general public use. *Id.* at 47. In addition, the dissent criticized the majority for hastily concluding that thermal images were not in general public use without discussing the prevalence of thermal image devices. *Id.*; *see* Douglas Adkins, Note, *The Supreme Court Announces a Fourth Amendment "General Public Use" Standard for Emerging Technologies but Fails to Define It:* Kyllo v. United States, 27 U. DAYTON L. REV. 245, 252–67 (2002) (criticizing the "general public use" doctrine).

[56] *Kyllo*, 533 U.S at 36. The Court rejected the dissent's argument that information revealed by an inference could not be considered a search. *Id.*

[57] *Id.*

[58] *Id.* at 35.

[59] *See Carpenter*, 138 S. Ct. at 2222 (holding that a warrant is required in the "rare case" where a person has Fourth Amendment rights in data held by a third party).

[60] NIST SMART GRID REPORT, *supra* note 7, at 11. *But see Naperville*, 900 F.3d at 527 (finding that the public utility was not a third party because the information flowed directly from the citizens to the utility).

[61] Robert M. Bloom & William T. Clark, *Small Cells, Big Problems: The Increasing Precision of Cell Site Location Information and the Need for Fourth Amendment Protections*, 106 J. CRIM. L. & CRIMINOLOGY 167, 178, 181 (2016).

[62] *Smith*, 442 U.S. at 743–44; *Miller*, 425 U.S. at 443.

[63] Kerr, *Case for the Third-Party Doctrine*, *supra* note 15, at 567–69; *see* United States v. White, 401 U.S. 745, 750 (1971) (involving a confession of crimes to a friend wearing a wire); Hoffa v. United States, 385 U.S. 293, 296 (1966) (addressing a person's incriminating statements to a co-worker

person's Fourth Amendment rights are not violated when a person voluntarily shares information with a government actor, even if the person does so unknowingly.[64] For example, in 1971, the Supreme Court considered whether the Fourth Amendment applied to self-incriminating statements that were made to an undercover informant in *United States v. White*.[65] There, the Court considered the *Katz* test.[66] A person should understand, the Court reasoned, that information disclosed to others could be relayed to the police.[67]

Between 1973 and 1980, courts used the third-party doctrine in cases involving business records.[68] For example, in 1976, the Supreme Court held in *United States v. Miller* that a person who deposits money into a bank has no legitimate expectation of privacy in the checks and deposit slips retained by the bank.[69] Similarly, in 1979, the Court held in *Smith v. Maryland* that, under

---

who was an undercover informant); Lewis v. United States, 385 U.S. 206, 210 (1966) (concerning a sale of marijuana to an undercover agent); Lopez v. United States, 373 U.S. 427, 435 (1963) (involving an attempt to bribe an Internal Revenue Service (IRS) agent); Lee v. United States, 343 U.S. 747, 757–58 (1952) (holding that the Fourth Amendment did not protect a person who made incriminating statements to a friend secretly working with the police).

[64] *See, e.g.*, *White*, 401 U.S. at 750 (holding that the third-party doctrine survived the *Katz* reasonable expectation of privacy test); *Hoffa*, 385 U.S. at 302 (noting that the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it"); *Lewis*, 385 U.S. at 210 (finding that an application of the Fourth Amendment to secret agent cases would impede undercover investigations).

[65] *White*, 401 U.S. at 752. In *White*, an informant had several conversations with the defendant while wearing a wire. *Id.* at 747. The U.S. Court of Appeals for the Seventh Circuit erroneously interpreted *Katz* as overruling *Lee*, an undercover agent case. *Id.* The Supreme Court reversed, emphasizing that *Katz* did not disrupt the principle in *Lee*: The Fourth Amendment does not protect voluntary statements made to others who turn out to be working with the government. *Id.* at 750.

[66] *Id.* at 750.

[67] *Id.* at 752.

[68] Kerr, *Case for the Third-Party Doctrine*, *supra* note 15, at 569–70; *see Smith*, 442 U.S. at 743–44 (phone records); *Miller*, 425 U.S. at 443 (bank records); Couch v. United States, 409 U.S. 322, 340 (1973) (tax documents). Some states offer stronger protections in business records when interpreting their own constitutions. *See, e.g.*, Burrows v. Superior Court, 529 P.2d 590, 593 (Cal. 1974) (holding that a person has a reasonable expectation of privacy in bank records); State v. Lunsford, 141 A.3d 270, 284 (N.J. 2016) (finding that "telephone billing records, [and] bank records . . . disclose private information that is entitled to constitutional protection"); Commonwealth v. Dejohn, 403 A.2d 1283, 1290 (Pa. 1979) (noting that the third-party doctrine "opens the door to a vast and unlimited range of very real abuses of police power").

[69] *Miller*, 425 U.S. at 443. There, the defendant argued that the collection of his bank records via a subpoena was a violation of his Fourth Amendment rights because he had a privacy interest in the documents. *Id.* at 442. The Court reasoned that a person assumes the risk that information handed over to a third party may be conveyed to the government. *Id.* at 443. Ultimately, the court extended the third-party doctrine, finding that:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Id.

the first prong of the *Katz* test, there is no subjective expectation of privacy in dialed telephone numbers, as the numbers are voluntarily conveyed to the telephone company.[70] Even if there were a subjective expectation of privacy, the Court held that, under the second prong of the *Katz* test, such an expectation was not one that society would recognize as reasonable.[71] In both cases, the Court also considered the nature of the information in the records.[72] In sum, business records were generally not entitled to Fourth Amendment protection due to the third-party doctrine.[73]

3. The "Rare" *Carpenter* Case

The Supreme Court in *Carpenter* held that police officers need a warrant to access cell-site location records.[74] In doing so, the Court limited the application of the third-party doctrine by refusing to apply the doctrine to records containing cell-site location information (CSLI).[75] Prior to *Carpenter*, courts had mechanically applied the third-party doctrine to all information voluntarily disclosed, such as information disclosed to an undercover police officer or a business.[76] Similarly, courts applied the third-party doctrine to CSLI to conclude that no Fourth Amendment search occurred.[77] In *Carpenter*, however,

---

[70] *Smith*, 442 U.S. at 743–44. There, the defendant was making obscene phone calls to a woman. *Id.* at 737. The police used a pen register, an electronic device that records phone numbers that are called from someone's phone, to reveal that the defendant was making the calls. *Id.* The Court held that the defendant did not have a reasonable expectation of privacy in the numbers he dialed from his phone because he provided that information to his cell phone provider, a third party. *Id.* at 743–44.

[71] *Id.* at 744.

[72] *See id.* at 741 (considering the information in the pen register and distinguishing it from the information obtained by the listening device in *Katz*); *Miller*, 425 U.S. at 442 (noting that *Katz* requires an inquiry into "the nature of the particular documents sought . . . to determine whether there is a legitimate 'expectation of privacy' concerning their contents").

[73] *See Smith*, 442 U.S. at 743–44 (holding that a person does not have a reasonable expectation of privacy in phone records); *Miller*, 425 U.S. at 443 (holding that a person does not have a reasonable expectation of privacy in bank records).

[74] *Carpenter*, 138 S. Ct. at 2222.

[75] *Id.*

[76] *See, e.g.*, Henderson v. State, 583 So. 2d 276 (Ala. Crim. App. 1990) (finding that a person has no reasonable expectation of privacy in phone records); Kesler v. State, 291 S.E.2d 497 (Ga. 1982) (denying Fourth Amendment protection to phone records); State v. Schultz, 850 P.2d 818 (Kan. 1993) (applying the third party-doctrine to telephone and bank records). *See generally* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U.L. REV. 373 (discussing states that have rejected the third-party doctrine).

[77] United States v. Graham, 824 F.3d 421, 435 (4th Cir. 2016) (explaining that the government does not need a warrant to access cell-site location information (CSLI) because "the very act of disclosure negated any reasonable expectation of privacy"); United States v. Davis, 785 F.3d 498, 531 (11th Cir. 2015) (finding that the privacy interest in CSLI is indistinguishable from the privacy interest in the phone records in *Smith*); *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 606 (5th Cir. 2013) (holding that law enforcement access to CSLI under the Stored Communications Act's "specific and articulable facts" standard, which is lower than the Fourth

the Court concluded that "the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[78]

In *Carpenter*, the Supreme Court limited the third-party doctrine in two ways.[79] First, the Court evaluated the privacy interests contained in the record sought by the government.[80] When a record discloses a "normal" amount of private information—such as a phone number—the third-party doctrine will likely still apply.[81] On the other hand, when records reveal information warranting increased privacy, or information beyond what society deems to be a "normal" amount, voluntary disclosure does not eliminate Fourth Amendment protections.[82] Prior to *Carpenter*, courts generally only looked to whether records were shared with a third party and did not necessarily consider the privacy interest in those records.[83] In *Carpenter*, the Supreme Court held that, because CSLI is functionally a "dossier of physical movements," it deserves the highest privacy protections.[84] In fact, the Court distinguished *Smith* and *Miller* on the basis that those cases involved only limited types of personal information.[85] The Court recognized that "seismic shifts in digital technology" can generate highly personal information in records, rendering such records more deserving of privacy protections than those in *Smith* and *Miller*.[86]

Amendment's probable cause standard, was not unconstitutional); State v. Perry, 776 S.E.2d 528, 542 (N.C. Ct. App. 2015) (concluding that the government's request for CSLI was not considered a Fourth Amendment search). *But see* State v. Andrews, 134 A.3d 324, 327 (Md. Ct. Spec. App. 2016) (holding that "people have a reasonable expectation that their cell phones will not be used as real-time tracking devices"); Commonwealth v. Augustine, 35 N.E.3d 688, 694 (Mass. 2015) (requiring a warrant for CSLI).

[78] *Carpenter*, 138 S. Ct. at 2223.

[79] *See id.* at 2217–20 (looking at the privacy interests and the voluntariness of the sharing of the information).

[80] *Id.* at 2217.

[81] *Id.*; *see, e.g.*, *Smith*, 442 U.S. at 743–44 (refusing to recognize Fourth Amendment rights in the numbers that the defendant dialed from his phone).

[82] *Carpenter*, 138 S. Ct. at 2217.

[83] *See Smith*, 442 U.S. at 743–44 (holding that a person does not have a reasonable expectation of privacy in phone records); *Miller*, 425 U.S. at 443 (holding that a person does not have a reasonable expectation of privacy in bank records); *Graham*, 824 F.3d at 425 (holding that voluntary disclosure of CSLI removes any reasonable expectation of privacy); *Davis*, 785 F.3d at 531 (finding that the defendant had a diminished expectation of privacy in CSLI records because a third party held the records).

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

[85] *Id.* at 2219.

[86] *Id.*; *see* Bloom & Clark, *supra* note 61, at 174–76 (discussing the rising popularity of small cell technologies which is enabling CSLI's accuracy). Specifically, CSLI can show a person's location within ten feet. *Id.* at 176. In contrast, GPS can show a person's location within fifty feet. *Id.*; Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 129 (2012).

Second, the Court also distinguished *Smith* and *Miller* based on how "voluntary" the sharing of information with a third party truly is.[87] CSLI can accumulate when a person is not actively using their phone, for example, when they receive a call, text, or email.[88] Additionally, CSLI is automatically generated when apps are checking the weather or social media updates.[89] As a result, anyone who owns a phone cannot avoid generating a log of places they have been.[90] Moreover, owning a phone is practically mandated as a condition of functioning in society.[91] This lack of affirmative action, the Court reasoned, is distinguishable from *Smith* and *Miller*.[92] In *Miller*, the defendant affirmatively decided to make bank deposits and write checks.[93] Likewise, in *Smith*, the defendant actively dialed the numbers on his phone.[94] Accordingly, the Court took a narrow view of voluntariness, explaining that someone does not voluntarily "assume the risk" of constant monitoring just by carrying a cellphone.[95] Because smart meter data is relayed to third parties, it is relevant to consider how law enforcement typically obtains data from third parties.[96]

B. The Legal Standard the Government Must Satisfy to Compel Records

Law enforcement agents typically use a subpoena or a warrant to obtain evidence.[97] A subpoena generally requires a showing of reasonableness, whereas a warrant requires a heightened showing of probable cause.[98] In the case of traditional energy meters, police have been successful in using subpoenas, rather

---

[87] *Carpenter*, 138 S. Ct. at 2220; *see* Bloom & Clark, *supra* note 61, at 196–99 (arguing that the third-party doctrine does not apply to CSLI because the sharing of the information with the cell phone provider is not truly voluntary).

[88] *Carpenter*, 138 S. Ct. at 2220. A cellular network utilizes cell towers equipped with antennas. Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. ATT'Y BULL., Nov. 2011, at 16, 19, 27 (2011). When a person's phone connects to a cell tower, a unique number identifies the phone. *Id.* at 20. The cell phone provider then uses this number for billing purposes. *Id.* at 23. CSLI comprises the resulting location and identifying information. *Id.*

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

[90] *Id.* To find this data on an iPhone, a person should: (1) go to the "settings" app on the iPhone, (2) scroll down and tap "privacy," (3) tap "location services" and scroll to the bottom of the screen, (4) tap "system services," and (5) scroll down to "significant locations." Fred Zahradnik, *How to Find Your Location History in Google Maps or iPhone*, LIFEWIRE (Nov. 8, 2019), https://www.lifewire.com/location-history-google-maps-iphone-1683392 [https://perma.cc/YT2D-9AXM].

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

[92] *Id.*

[93] *Miller*, 425 U.S. at 443.

[94] *Smith*, 442 U.S. at 743–44.

[95] *Carpenter*, 138 S. Ct. at 2220. The Court cautioned that their holding was narrow, only based on seven days of CSLI. *Id.*

[96] *See infra* notes 97–139 and accompanying text.

[97] *Carpenter*, 138 S. Ct. at 2222. *See generally* Robert M. Bloom, *Warrant Requirement—The Burger Court Approach*, 53 U. COLO. L. REV. 691 (1982) (recognizing the Burger Court's application of the *Katz* test as a deviation from the Warren Court's preference for the warrant requirement).

[98] Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 806–07 (2005).

than warrants, to gain access to data in marijuana growing operation investigations.[99] Subsection 1 of this Section discusses various standards for obtaining data.[100] Subsection 2 demonstrates how subpoenas have been used to compel utility companies to provide energy data to law enforcement.[101]

1. Investigative Tools: Warrants, Subpoenas, and Court Orders

In criminal investigations, the government may use a warrant or a subpoena to obtain evidence.[102] In most cases, when the government conducts a "search" under the Fourth Amendment, a warrant is required.[103] A warrant authorizes law enforcement officials to physically enter the place where evidence is believed to be and take evidence that they find.[104] In contrast, when the government uses a subpoena, it instructs a party to provide the government with the requested evidence.[105] The subpoena recipient must gather the evidence on its own and then provide it to the government.[106]

An important distinction between subpoenas and warrants is that warrants always require a showing of probable cause, whereas subpoenas require a lower burden of proof.[107] Probable cause exists where there is a reasonable belief that evidence of criminal activity will be found.[108] When law enforcement agents use a warrant, a search occurs and a person can challenge the validity of

---

[99] *See* United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1117 (9th Cir. 2012) (upholding the Drug Enforcement Administration's subpoena for energy consumption records in an investigation of illegal use and distribution of marijuana); United States v. Hoang, 487 F. App'x 239, 245 (6th Cir. 2012) (finding that utility records supported probable cause for the search of defendant's home); *McIntyre*, 646 F.3d at 1111 (upholding the county attorney's subpoena of electricity usage records in drug crime investigation involving marijuana).

[100] *See infra* notes 102–120 and accompanying text.

[101] *See infra* notes 121–139 and accompanying text.

[102] Slobogin, *supra* note 98, at 810. When the government seeks records, a subpoena is generally the preferred mechanism. *Id.*

[103] *See, e.g.*, Birchfield v. North Dakota, 136 S. Ct. 2160, 2173 (2016) (noting that police must obtain a warrant prior to conducting a search); Kentucky v. King, 563 U.S. 452, 459 (2011) ("[T]his Court has inferred that a warrant must generally be secured."); *see also* Timothy Andrea, *The Exigencies of Drunk Driving:* Cripps v. State *and the Issues with Taking Drivers' Blood Without a Warrant*, 59 B.C. L. REV. E. SUPP. 482, 484–85 (2018) (summarizing the warrant requirement and the exigent circumstances exception).

[104] Slobogin, *supra* note 98, at 810; Orin Kerr, *Does* Carpenter *Revolutionize the Law of Subpoenas?*, LAWFARE (June 26, 2018), https://www.lawfareblog.com/does-carpenter-revolutionize-law-subpoenas [https://perma.cc/G5TS-V2BV] [hereinafter Kerr, *The Law of Subpoenas*].

[105] Slobogin, *supra* note 98, at 810.

[106] *See Carpenter*, 138 S. Ct. at 2250–57 (Alito, J., dissenting) (discussing the history of subpoenas in the United States).

[107] *See* U.S. CONST. amend. IV (noting that "no Warrants shall issue, but upon probable cause"); United States v. R. Enters., Inc., 498 U.S. 292, 297 (1991) (finding that a grand jury subpoena does not require probable cause "because the very purpose of requesting the information is to ascertain whether probable cause exists").

[108] BLOOM & BRODIN, *supra* note 37, at 121. A valid search warrant must also describe the place to be searched and the items sought with particularity. *Id.* at 123.

the warrant or the search on Fourth Amendment grounds.[109] On the other hand, when law enforcement agents use a subpoena, the Fourth Amendment is not strongly implicated because police are not physically taking evidence.[110] Instead, a person can challenge the subpoena on Fifth Amendment grounds, but this is rarely successful.[111] There are two types of subpoenas that may require an individual to turn over evidence to law enforcement: a subpoena *duces tecum* and an administrative subpoena.[112] A grand jury or prosecutor manages a subpoena *duces tecum*, which requires a suspect to appear before the court and produce evidence.[113] A government agency, in contrast, administers an administrative subpoena.[114]

The government can also seek to obtain information through a court order.[115] In *Carpenter*, for example, the government seized the defendant's CSLI under the Stored Communications Act (SCA).[116] The SCA authorizes the government to obtain information through a warrant, an administrative subpoena,

---

[109] *Id.* at 121. To challenge a warrant, a person can argue that police officers did not have probable cause. United States v. Leon, 468 U.S. 897, 900 (1984). Alternatively, a person could argue that police officers exceeded the scope of the warrant. Maryland v. Garrison, 480 U.S. 79, 88 (1987). To challenge a search based on the Fourth Amendment, a person can argue that police officers needed a warrant. BLOOM & BRODIN, *supra* note 37, at 121. To preserve the element of surprise, a warrant can be issued without prior notice. Marshall v. Barlow's, Inc., 436 U.S. 307, 316 (1978); United States v. Bailey (*In re* Subpoena Duces Tecum), 228 F.3d 341, 348 (4th Cir. 2000).

[110] Slobogin, *supra* note 98, at 807.

[111] *Id.* at 813. Challenging a subpoena based on the Fifth Amendment is usually futile. *Id.* at 806. A person could also resist a subpoena based on burdensomeness and irrelevance. *Id.* Arguing that a subpoena is too burdensome, however, is "almost always doomed to failure." WAYNE R. LAFAVE ET AL., 3 CRIM. PROC. 135 (2d ed. 1999). Challenging a subpoena because it is irrelevant is also difficult. Slobogin, *supra* note 98, at 806. For example, grand jury subpoenas are deemed irrelevant only when "there is no reasonable possibility that the category of materials the government seeks will produce information relevant to the general subject of the grand jury's investigation." *R. Enters., Inc.*, 489 U.S. at 301. Similarly, there is a relatively low threshold for proving relevance in the case of administrative subpoenas. Slobogin, *supra* note 98, at 806.

[112] U.S. DEP'T OF JUSTICE, CRIMINAL RESOURCE MANUAL 408 (2018); Slobogin, *supra* note 98, at 805. A grand jury subpoena requires an individual to bring evidence to a grand jury proceeding. U.S. DEP'T OF JUSTICE, *supra*, at 408.

[113] Slobogin, *supra* note 97, at 805–06.

[114] U.S. DEP'T OF JUSTICE, *supra* note 112, at 408. To be constitutional, administrative subpoenas must also only be used where the government does not already have the information and enforcing the subpoena will not be an abuse of the court system. CHARLES DOYLE, CONG. RESEARCH SERV., RL33321, ADMINISTRATIVE SUBPOENAS IN CRIMINAL INVESTIGATIONS: A BRIEF LEGAL ANALYSIS 1 (2006) [hereinafter CRS ADMINISTRATIVE SUBPOENAS REPORT].

[115] *See Carpenter*, 138 S. Ct. at 2210 (obtaining CSLI data pursuant to a court order). *See generally* Claudia G. Catalano, Annotation, *Criminal Defendant's Rights Under Stored Communications Act, 18 U.S.C.A. §§ 2701 et seq.*, 11 A.L.R. Fed. 3d Art. 1 (2016) (summarizing the SCA).

[116] *Carpenter*, 138 S. Ct. at 2210; *see* Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it*, 72 GEO. WASH. L. REV. 1208, 1218 (2004) (explaining the compelled disclosure rules in the SCA) [hereinafter Kerr, *A User's Guide to the SCA*]. The SCA makes it illegal to access or disclose stored electronic communications records, unless the government compels such disclosure as allowed by the statute. 18 U.S.C. § 2703 (2018). *See generally* Catalano, *supra* note 115 (examining a defendant's rights under the SCA).

or a § 2703(d) court order.[117] In *Carpenter*, the Federal Bureau of Investigation (FBI) used a court order, which required the government to show reasonable grounds for believing that the records were "relevant and material to an ongoing investigation."[118] This standard has been described as "a mix between a subpoena and a search warrant."[119] Though warrants, subpoenas, and court orders may provide access to data, a subpoena has been the primary mechanism for compelling the disclosure of traditional energy meter data.[120]

2. Use of Subpoenas to Access Traditional Energy Meter Data

Utility records have been an important part of law enforcement investigations involving drug crimes.[121] Historically, law enforcement agents did not need a warrant to access energy consumption data.[122] For example, in 2012,

---

[117] 18 U.S.C. § 2703(b)(1)(B)(ii).

[118] *Id.* § 2703(d). Section 2703(d) court orders require notifying the person whose records are sought. *Id.* § 2705. The judge will issue the order if the government makes the requisite showing. Kerr, *A User's Guide to the SCA*, *supra* note 116, at 1218. Once the order is issued, it is served like an ordinary subpoena. *Id.*

[119] Kerr, *A User's Guide to the SCA*, *supra* note 116, at 1219.

[120] Jack I. Lerner & Deirdre K. Mulligan, *Taking the "Long View" on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3, 33.

[121] *See Golden Valley Elec. Ass'n*, 689 F.3d at 1117 (upholding the Drug Enforcement Administration's subpoena for energy consumption records in an investigation of illegal use and distribution of marijuana); *Hoang*, 487 F. App'x at 245 (concluding utility records supported probable cause for the search of defendant's home); *McIntyre*, 646 F.3d at 1111 (upholding the county attorney's subpoena of electricity usage records in drug crime investigation involving marijuana); United States v. Thomas, 605 F.3d 300, 306 (6th Cir. 2010) (finding that utility records could refresh a 'stale' tip from a confidential informant to support probable cause); United States v. Hamilton, 434 F. Supp. 2d 974, 987 (D. Or. 2006) (determining that there is no reasonable expectation of privacy in home power consumption data obtained via administrative subpoena). In 1994, in *United States v. Field*, a deputy sheriff executed a subpoena *duces tecum* on an electricity company to obtain electric bills. 855 F. Supp. 1518, 1523 (W.D. Wis. 1994). There, the defendant was suspected of growing marijuana and the sheriff sought to determine whether the defendant's electrical use was high. *Id.*

[122] *Golden Valley Elec. Ass'n*, 689 F.3d at 1117. Electric utilities may also voluntarily disclose electric bills to law enforcement, who can then use the information as the basis for search warrants. Dean Narciso, *Police Seek Utility Data for Homes of Marijuana Growing Suspects*, COLUMBUS DISPATCH (Feb. 28, 2011), https://www.dispatch.com/article/20110228/NEWS/302289766 [https://perma.cc/W3W2-Y2BS] (explaining that if no illegal behavior is observed at a person's home, police might seek access to energy records in order to support a search warrant). Some have pondered why utility companies would want to report their "best customers" to law enforcement, speculating that utility companies might have a financial incentive to do so. The Weed Blog, *Do Utilities Tell Cops About Marijuana Gardens with High Electricity Bills?*, CANNABIS MAVEN (Jan. 29, 2012), https://cannabismaven.io/theweedblog/policies/do-utilities-tell-cops-about-marijuana-gardens-with-high-electricity-bills-ABXPziugNkCts8G0TwslZw/ [https://perma.cc/FX5B-F9VH]. In California, for example, a utility company alerted law enforcement to an abnormally high electric bill. *A Suspicious Electric Bill?*, PRIVACY.ORG (Mar. 29, 2004), https://privacy.org/archives/001250.html [https://perma.cc/C8X3-W5PV]. Law enforcement investigated the home for involvement in marijuana production. *Id.* Ultimately, the family simply used a large amount of electricity. *Id.*; *see* Balough, *supra* note 5, at 172 (noting that "there is a history of voluntary utility compliance with government requests to share personal consumer usage information, such as by the phone companies after 9/11").

the United States Court of Appeals for the Ninth Circuit upheld warrantless access to energy consumption records in *United States vs. Golden Valley Electric Ass'n*.[123] In *Golden Valley*, the Drug Enforcement Administration subpoenaed electricity records of three homes.[124] The utility company challenged the subpoena.[125] Ultimately, the Ninth Circuit held that individuals do not have a reasonable expectation of privacy in a business record owned by the utility company.[126]

The third-party doctrine has successfully allowed law enforcement to bypass the warrant requirement when investigating marijuana growers.[127] For example, as early as 1993, the Idaho Court of Appeals applied the third-party doctrine in holding that the Fourth Amendment did not apply to power records.[128] Power records are business records, the court reasoned, and *Miller* and *Smith* recognized that the Fourth Amendment did not protect business records.[129] Though the Fourth Amendment did not apply, the court proceeded to evaluate the privacy interest in the power records in determining whether the Idaho Constitution protected the records.[130] To determine the privacy interest, the court applied the *Katz* test.[131] The court noted that the records only revealed power usage, did not identify the defendant's activities, and did not reveal any intimate information.[132] The court reasoned that various factors could

---

[123] *Golden Valley Elec. Ass'n*, 689 F.3d at 1117.

[124] *Id.* The Drug Enforcement Administration served an administrative subpoena on Golden Valley, the electric utility. *Id.* at 1111. Specifically, the Comprehensive Drug Abuse Prevention and Control Act of 1970 gives the Attorney General the authority to utilize administrative subpoenas in connection with drug crime investigations. *Id.* at 1113 (citing 21 U.S.C. § 876(a) (2018)).

[125] *Id.* at 1114.

[126] *Id.* at 1116. Golden Valley asserted the Fourth Amendment claim on behalf of its consumers. *Id.* The Ninth Circuit was not convinced that Golden Valley had the authority to do so but did not address the question due to the third-party doctrine. *Id.*

[127] *McIntyre*, 646 F.3d at 1111. In *Golden Valley*, the Ninth Circuit did not explicitly apply the third-party doctrine but cited to *Smith* and *Miller* in holding that a person has no reasonable expectation of privacy in energy consumption records. *Golden Valley Elec. Ass'n*, 689 F.3d at 1117.

[128] Idaho v. Kluss, 867 P.2d 247, 252 (Idaho Ct. App. 1993); *see Hamilton*, 434 F. Supp. 2d at 980 (finding that a person has no expectation of privacy in electricity consumption records).

[129] *Kluss*, 867 P.2d at 252; *see Smith*, 442 U.S. at 743–44 (holding that a person has no reasonable expectation in phone records); *Miller*, 425 U.S. at 443 (holding that a person has no reasonable expectation in bank records); *Couch*, 409 U.S. at 340 (1973) (holding that a person has no reasonable expectation in tax records); *see also* Erin Murphy, *The Case Against the Case for the Third Party Doctrine*, 24 BERKELEY TECH. L.J. 1239, 1252 (2009) (advocating for a balancing test to determine whether a person forfeits privacy in records); James M. Small, *Storing Documents in the Cloud: Toward an Evidentiary Privilege Protecting Papers and Effects Stored on the Internet*, 23 GEO. MASON U. CIV. RTS. L.J. 255, 264–67 (2013) (discussing the third-party doctrine in connection with business records).

[130] *Kluss*, 867 P.2d at 252.

[131] *Id.* at 253.

[132] *Id.* at 254. In addition, the court said that the privacy expectation is even lower in power records than in bank or telephone records, which reveal information about a person's activities. *Id.* The defendant relied on *People v. Chapman*, 679 P.2d 62 (1984), where the court determined that a person

cause a person to consume large amounts of power such as having a hot tub or poor insulation.[133] Because the cause of a high power bill is not immediately clear from the bill itself, the court concluded that, under *Katz*, society would not reasonably recognize a person's privacy interests in power records.[134]

Similarly, in 2011, the United States Court of Appeals for the Eighth Circuit upheld an administrative subpoena used to obtain electricity usage records based on the third-party doctrine in *United States v. McIntyre*.[135] In *McIntyre*, the defendant argued that a warrant was required to access his energy records because it revealed "intimate details about the interior of his home."[136] Namely, the defendant relied on *Kyllo* to argue that the inference made from the energy consumption record was the same inference that was made in *Kyllo*: high-energy usage is consistent with a marijuana grow light.[137] The Eight Circuit, however, found that police use of a thermal image device in *Kyllo* was different than merely asking the utility company for records.[138] Put differently, because the electricity records were compelled via a subpoena, and the information was not gathered directly by law enforcement, there was significantly less intrusion into a person's reasonable expectation of privacy.[139]

---

had a reasonable expectation of privacy in his unlisted phone number. *Kluss*, 867 P.2d at 253. In *Chapman*, the defendant paid an extra fee to the telephone company to obtain an unlisted telephone number. 679 P.2d at 68. There, the court held that the "disclosure of the subscriber's name and address may well add the missing link to make up a 'virtual current biography.'" *Id.* at 68–69 (quoting *Burrows*, 529 P.2d at 596 (1974)). The court in *Kluss*, however, distinguished *Chapman* on the grounds that electric utility records did not "provide or complete a 'virtual current biography.'" *Kluss*, 867 P.2d at 253–54.

[133] *Kluss*, 867 P.2d at 254.

[134] *Id.*

[135] *McIntyre*, 646 F.3d at 1111. An administrative subpoena can be challenged on the grounds that it is "too indefinite or broad." Peters v. United States, 853 F.2d 692, 699 (9th Cir. 1988). Ultimately, an administrative subpoena will be upheld if (1) Congress has granted the administration the authority to investigate; (2) appropriate procedures were followed; and (3) the evidence sought is relevant to an ongoing investigation. *Investigation and Police Practices, Overview of the Fourth Amendment*, 35 GEO. L.J. ANN. REV. CRIM. PROC. 3, 114–16 (2006). The U.S. Court of Appeals for the Ninth Circuit has held that a "Fourth Amendment 'reasonableness' inquiry must also be satisfied" when evaluating an administrative subpoena. Reich v. Mont. Sulphur & Chem. Co., 32 F.3d 440, 444 n.5 (9th Cir. 1994).

[136] *McIntyre*, 646 F.3d at 1111.

[137] *Id.*

[138] *Id.*; *see* United States v. Starkweather, No. 91-30354, 1992 U.S. App. LEXIS 20207, at *4 (9th Cir. Aug. 24, 1992) (finding that there is no reasonable expectation of privacy in electric utility records because the records were similar to bank and phone records).

[139] *McIntyre*, 646 F.3d at 1111; *see Carpenter*, 138 S. Ct. at 2247 (Alito, J., dissenting) (explaining that there is a "basic distinction between an actual search . . . and an order merely requiring a party to look through its own records and produce specified documents" and that "[t]he former, which intrudes on personal privacy far more deeply, requires probable cause," and "the latter does not").

II. *CARPENTER*'S RECOGNITION OF FOURTH AMENDMENT RIGHTS IN RECORDS HELD BY A THIRD PARTY

This Part discusses the 2018 U.S. Supreme Court decision in *Carpenter v. United States*.[140] Section A of this Part explains how third-party storage of data resulted in a Fourth Amendment void pre-*Carpenter*.[141] Section B summarizes the facts and holding of *Carpenter*.[142] Section C explains how *Carpenter* resolved the gap in Fourth Amendment jurisprudence by requiring law enforcement to obtain a warrant prior to requesting data held by a third party.[143]

A. Pre-Carpenter Confusion: What Legal Standard Governs Access to Records Stored by a Third Party in Which a Person Has Fourth Amendment Rights?

The standard to apply when law enforcement seeks to obtain remotely stored records in which a person has Fourth Amendment rights was unclear prior to *Carpenter*.[144] To obtain evidence stored with a third party, law enforcement could use a warrant or a subpoena.[145] Using a warrant in this way, however, is impractical.[146] A warrant enables police to storm into a company's headquarters and search company servers to obtain information on just one individual.[147] This non-sensical approach is often unnecessary because third party providers are generally willing to turn over the data.[148]

---

[140] *See infra* notes 143–184 and accompanying text.

[141] *See infra* notes 144–157 and accompanying text.

[142] *See infra* notes 158–172 and accompanying text.

[143] *See infra* notes 171–185 and accompanying text.

[144] Kerr, *The Law of Subpoenas*, *supra* note 104; *see* United States v. Barr, 605 F. Supp. 114, 119 (S.D.N.Y. 1985) (upholding initial warrant to access mail box, and subsequently upholding a subpoena to compel an individual to hand over the documents in the mail box). In *Barr*, the court left open the question of whether a subpoena could be used to open the documents in the mailbox without the need for a warrant. *Id.*; Kerr, *The Law of Subpoenas*, *supra* note 104. In other cases, the court held that a warrant is required to access data. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that a user has Fourth Amendment rights in the contents of their remotely stored email and therefore a warrant is required); United States v. Bach, 310 F.3d 1063, 1066 n.1 (8th Cir. 2002) (noting, that the court "analyze[s] this case [about access to remotely stored emails] under the search warrant standard, not under the subpoena standard"); Doe v. Broderick, 225 F.3d 440, 454 (4th Cir. 2000) (requiring a warrant to access medical records); Louisiana v. Skinner, 10 So. 3d 1212, 1213 (La. 2009) (holding that a warrant is necessary to access prescription records). *But see* Commonwealth v. Riedel, 651 A.2d 135, 140 (Pa. 1994) (holding that a person has a reasonable expectation of privacy in medical records and requiring a showing of probable cause but not requiring a warrant).

[145] Slobogin, *supra* note 98, at 806; Kerr, *The Law of Subpoenas*, *supra* note 104.

[146] Kerr, *The Law of Subpoenas*, *supra* note 104.

[147] *Id.*

[148] *Id.*

Law enforcement traditionally use a subpoena to access data held by third parties.[149] If a person has Fourth Amendment rights in the data to be seized, however, the use of a subpoena would render those Fourth Amendment rights meaningless.[150] Law enforcement could simply subpoena records without satisfying the Fourth Amendment's probable cause requirement.[151] Moreover, a person could not challenge the subpoena based on the Fifth Amendment because the records are kept with a third party.[152] So, the use of a subpoena to access such records allows law enforcement to bypass Fourth Amendment rights and leaves people unprotected by the Fifth Amendment.[153]

Before *Carpenter*, courts had rarely addressed this issue due to the third-party doctrine.[154] The third-party doctrine recognizes that a person does not have Fourth Amendment rights in certain records.[155] Therefore, without first recognizing that a person has Fourth Amendment rights, it is unnecessary to decide the standard needed to gain access to data in which a person has such rights.[156] This is the issue that the Supreme Court confronted in *Carpenter*.[157]

---

[149] *Id.*; *see supra* notes 121–139 and accompanying text. Additionally, by subpoenaing a record from a third party, police could avoid the risk that a person might destroy the record. A.B.A. STANDARDS FOR CRIMINAL JUSTICE, LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS 4 (2012).

[150] Kerr, *The Law of Subpoenas*, *supra* note 104.

[151] *Id.*

[152] *See generally* Robert P. Mosteller, *Simplifying Subpoena Law: Taking the Fifth Amendment Seriously*, 73 VA. L. REV. 1 (1987) (explaining that third parties have "constructive possession" of records, and as such are not subject to the Fifth Amendment). In 1976, in *Fisher v. United States*, the Supreme Court held that the Fifth Amendment right against self-incrimination did not protect against a subpoena for tax records. 425 U.S. 391, 410 (1976). One commentator has interpreted *Fisher* as creating a "framework of a new system in which the availability of the privilege turns, apparently exclusively, upon whether the act of production involves testimonial self-incrimination." Mosteller, *supra*, at 5.

[153] Kerr, *The Law of Subpoenas*, *supra* note 104. The Supreme Court recognized this conundrum in *SEC v. Jerry T. O'Brien, Inc.* 467 U.S. 735, 742–43 (1984). There, the Court explained:

> [A] person inculpated by materials sought by a subpoena issued to a third party cannot seek shelter in the Self-Incrimination Clause of the Fifth Amendment . . . . It is established that, when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities.

Id. at 742–43.

[154] Kerr, *The Law of Subpoenas*, *supra* note 104; *see* Carpenter v. United States, 138 S. Ct. 2206, 2555 (2018) (Alito, J., dissenting) (noting that "the reason that we have never seen such a case is because—until today—defendants categorically had no 'reasonable expectation of privacy' and no property interest in records belonging to third parties").

[155] Kerr, *The Law of Subpoenas*, *supra* note 104.

[156] *See generally* Brief of Amicus Curiae Professor Orin S. Kerr at 15–26, United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238) (urging the court to consider whether the Fourth Amendment should be evaluated under search warrant precedents or subpoena precedents).

[157] *Carpenter*, 138 S. Ct. at 2222.

B. Facts and Holding of Carpenter v. United States

In *Carpenter*, the FBI suspected several men of committing group robberies in Michigan and Ohio.[158] To prove that Timothy Carpenter, one of the suspects, was near the stores when the crimes occurred, the FBI sought Carpenter's cell phone records.[159] Specifically, the FBI applied for a § 2703(d) order under the SCA and requested CSLI for a four-month period.[160] CLSI is generated every time a phone connects to a cell-site, which may happen several times per minute even if a person is not using their phone.[161] The CSLI taken from Carpenter's phone confirmed that Carpenter was near the stores at the exact time the robberies took place.[162] Determining whether the government's request for CSLI constituted a Fourth Amendment search, the U.S. Court of Appeals for the Sixth Circuit applied the third-party doctrine and held that cell phone records were business records not entitled to Fourth Amendment protections.[163] The Supreme Court reversed, finding that a person has a reasonable expectation of privacy in CSLI.[164]

Recognizing that CSLI data requires a warrant, Chief Justice John G. Roberts, Jr., writing for the majority, emphasized that CSLI provides a complete record of a person's travel history.[165] Evaluating the intrusiveness of the data, he highlighted that "time-stamped data provides an intimate window into

---

[158] *Id.* at 2212. Police officers arrested four men for robbing Radio Shack and T-Mobile stores in Detroit, Michigan. *Id.* One of the men implicated fifteen accomplices and provided the FBI with their cell phone numbers. *Id.*

[159] *Id.* After obtaining the CSLI from MetroPCS and Sprint, the government amassed 12,989 location points showing Carpenter's movements. *Id.* This is the equivalent of 101 location data points per day. *Id.*

[160] 18 U.S.C. § 2703(d) (2018); *Carpenter*, 138 S. Ct. at 2212; *see supra* note 120 and accompanying text (explaining that a § 2703(d) order is a court order that functions like a subpoena); *supra* notes 116–120 and accompanying text (discussing the Stored Communications Act (SCA)). *See generally* Catalano, *supra* note 115 (explaining a defendant's rights under the SCA).

[161] *Carpenter*, 138 S. Ct. at 2220. In addition, seven of Carpenter's accomplices testified that he was the "leader." *Id.* at 2212.

[162] *Id.* at 2213; *see* Bloom & Clark, *supra* note 61, at 174–76 (discussing the science behind CSLI and the nature of the data). Specifically, CSLI can show a person's location within ten feet. *Id.* at 176. When a person's phone connects to a cell tower, it "pings," and a unique number identifies it. O'Malley, *supra* note 88, at 22–23. Cell phone providers then use this number to bill the user but links the person to the place the phone was when it pinged. *Id.* at 23. Cell-sites can be found on cell towers, light posts, flagpoles, or even on sides of buildings. *Carpenter*, 138 S. Ct. at 2211. Moreover, wireless carriers have installed more cell-sites to keep up with cell phone usage data. *Id.* at 2212. Naturally, with more cell-sites, it is easier to narrow down a person's location. Bloom & Clark, *supra* note 61, at 175.

[163] United States v. Carpenter, 819 F.3d 880, 889 (6th Cir. 2016) (holding that CSLI are "business records obtained from a third party, which can only diminish the defendants' expectation of privacy in the information those records contain").

[164] *Carpenter*, 138 S. Ct. at 2223.

[165] *Id.* at 2217.

a person's life."[166] Additionally, the majority pointed out that everyone has CSLI, not just those under investigation.[167] As a result, the government can essentially time-travel to track a person's past movements.[168] The Court explained that the only limit on collecting this data is the retention period imposed by cell phone carriers, which is typically five years.[169] Moreover, the Court found the large quantity of data points and the precision of the data to warrant a heightened privacy interest.[170] Ultimately, the Supreme Court held that the government conducts a search for Fourth Amendment purposes when it collects an individual's CSLI.[171] The next issue the Court addressed was the legal standard required for government access to records in which a person has Fourth Amendment rights.[172]

C. The Subpoena Analysis in Carpenter v. United States

In *Carpenter*, law enforcement obtained the defendant's cell-site data pursuant to a court order authorized by the SCA.[173] The Court held that the SCA's requirement that the information was "relevant and material to an ongoing investigation" was too far below the probable cause standard required by the Fourth Amendment.[174] Ultimately, the Court held that, just as in a local search, seeking access to information in which a person retains Fourth Amendment rights requires a warrant.[175]

---

[166] *Id.*

[167] *Id.* at 2218. The Court distinguished this situation from the one in *United States v. Jones*, where police attached a GPS tracking device to the defendant's car. *Id.* In *Jones*, the Court found the attachment of a GPS device to the defendant's car to be a search. 565 U. S. 400, 402 (2012). Notably, Justice Sotomayor joined the majority opinion, but wrote separately to express the dangers of location tracking. *Id.* at 413–18 (Sotomayor, J., concurring). Justice Sotomayor noted that GPS data was "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." *Id.* at 415.

[168] *Carpenter*, 138 S. Ct. at 2210.

[169] *Id.* at 2218. In *Jones*, Justice Sotomayor expressed concerns over the fact that GPS data can be held indefinitely. 565 U. S. 400 at 412 (Sotomayor, J., concurring).

[170] *Carpenter*, 138 S. Ct. at 2219. Specifically, CSLI can generate hundreds of data points that each pinpoint a person's location within 50 meters. *Id.*

[171] *Id.* at 2220. This is true at least when the CSLI meets the facts of *Carpenter* where a warrant was required to obtain more than six days of CSLI records. *See id.* (cautioning that the Court's holding "is a narrow one").

[172] *Id.* at 2221.

[173] *Id.*

[174] *Id.* According to the dissent's characterization of the majority's view, the Court held that "the Government crosses a constitutional line when it obtains a court's approval to issue a subpoena for more than six days of cell-site records in order to determine whether a person was within several hundred city blocks of a crime scene." *Id.* at 2224. (Kennedy, J., dissenting).

[175] *See id.* at 2221 (majority opinion) (noting that the "Government's obligation is a familiar one—get a warrant"). *But see* United States v. Poller, 43 F.2d 911, 914 (2d Cir. 1930) (noting that "the real evil aimed at by the Fourth Amendment is the search itself, that invasion of a man's privacy

In his dissent, Justice Alito wrote that the warrant requirement should not apply when the government seeks to obtain records using a subpoena, which makes use of a reasonableness standard.[176] Justice Alito found the fact that records are stored with a third party to be significant.[177] Specifically, he asserted that the risk of intrusion on privacy is much lower when records are being compelled than when they are being physically taken, as is the case with a typical search of the home.[178] Ultimately, Justice Alito noted that only cases of *actual* searches and seizures had ever invoked the warrant requirement.[179] Put differently, Justice Alito emphasized that there is a legally significant difference between law enforcement officials asking for records and law enforcement officials physically collecting the records.[180]

In response to Justice Alito, Chief Justice Roberts emphasized that CSLI is fundamentally different than other types of business records traditionally subject to a subpoena.[181] Moreover, the majority reasoned that the subpoena's reasonableness requirement is not enough to safeguard Fourth Amendment rights because law enforcement agents could subpoena records "for no reason other than 'official curiosity.'"[182] In sum, the Court held that if there is a constitutionally protectable privacy interest in records held by a third party, a warrant is required.[183] But this is a "rare case," according to the Court.[184] Nonethe-

---

which consists in *rummaging about among his effects* to secure evidence against him") (emphasis added).

[176] *Carpenter*, 138 S. Ct. at 2250–57 (Alito, J., dissenting); *see* Marty Lederman, Carpenter*'s Curiosities (and its Potential to Unsettle Longstanding Fourth Amendment Doctrines)*, BALKINIZATION (June 26, 2018), https://balkin.blogspot.com/2018/06/carpenter-s-curiosities-and-its.html [https://perma.cc/2J4F-4PFW] (noting that Justice Alito spent seventeen pages discussing the differences between a subpoena and a warrant).

[177] *Carpenter*, 138 S. Ct. at 2250–57 (Alito, J., dissenting).

[178] *Id.* at 2251–52. Justice Alito quoted Justice Brandeis, who was known to advocate for a liberal interpretation of the Fourth Amendment. *Id.* at 2251. *See generally* Warren & Brandeis, *supra* note 1, at 195 (discussing the "right to be let alone"). Notably, Justice Brandeis found that "there is no 'search' or 'seizure' when a defendant is required to produce a document in the orderly process of a court's procedure." Olmstead v. United States, 277 U.S. 438, 476 (1928) (Brandeis, J., dissenting).

[179] *Carpenter*, 138 S. Ct. at 2254 (Alito, J., dissenting).

[180] *Id.* at 2251–52. By applying the warrant requirement to constructive searches, or searches that do not require a physical intrusion, Justice Alito characterized the majority's holding as "revolutionary" and ignorant of "more than a century of Supreme Court precedent." *Id.* at 2247.

[181] *Id.* at 2222 (majority opinion). Justice Roberts noted that "CSLI is an entirely different species of business record—something that implicates basic *Fourth Amendment* concerns about arbitrary government power much more directly than corporate tax or payroll ledgers." *Id.*

[182] *Id.*

[183] *Id. Carpenter* left unanswered many questions about how a warrant would be effectuated in practice. *See* Kerr, *The Law of Subpoenas*, *supra* note 104 (finding that it might be difficult to apply the warrant requirement when a third party is holding the data). For example, Orin Kerr asks whether the burden is on the third party to determine whether a subpoena is asking for information in which a person has Fourth Amendment rights. *Id.*

[184] *Carpenter*, 138 S. Ct. at 2222.

less, courts are now free to examine whether smart meter data is a "rare case" envisioned by the Court in *Carpenter*.[185]

III. SMART METER DATA AND *NAPERVILLE SMART METER AWARENESS V. CITY OF NAPERVILLE*

In 2018, in *Naperville Smart Meter Awareness v. City of Naperville*, the United States Court of Appeals for the Seventh Circuit held that a public utility's collection of smart meter data is a reasonable search under the Fourth Amendment.[186] Notably, the Seventh Circuit highlighted that smart meter data can reveal significant information about what activities occur inside a person's home.[187] This Part explains the Seventh Circuit's decision in *Naperville*.[188] Section A of this Part discusses smart meter data and what it can reveal about a person's activities in the home.[189] Section B summarizes *Naperville*'s holding that smart meter data is protected by the Fourth Amendment.[190] Section C discusses *Naperville* in connection with the third-party doctrine.[191]

---

[185] *See supra* notes 158–184 and accompanying text.

[186] Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 529 (7th Cir. 2018). The lower court, the U.S. District Court for the Northern District of Illinois, dismissed the Fourth Amendment claim. Smart Meter Awareness v. City of Naperville, 69 F. Supp. 3d 830, 841 (N.D. Ill. 2014) (*Naperville I*). The court held that there was no reasonable expectation of privacy in smart meter data and thus, the data was not entitled to Fourth Amendment protection. *Id.* The court reasoned that because the data resulted in inferences that someone walking on the sidewalk could have made, there was no reasonable privacy interest. *Id.* Specifically, the court noted that if peak usage was shown around 7:00 pm:

> At most, someone inspecting the data might guess that at least one resident had been home at 7:00 pm. But that same guess could also be reasonably made by any member of the public walking by the residence who notices a car in the driveway or lights in the windows—that is not information that can be reasonably expected to remain private.

Id.

[187] *Naperville*, 900 F.3d at 526. Specifically, the court looked at studies demonstrating the types of information that smart meter data can reveal. *Id.* at 526 n.5. Orin Kerr criticized the *Naperville* court for accepting the conclusions of the studies as true despite the lack of evidence in the court record. Orin Kerr, *Public Utility's Recording of Home Energy Consumption Every 15 Minutes Is a 'Search,' Seventh Circuit Rules*, LAWFARE (Aug. 17, 2018), https://www.lawfareblog.com/public-utilitys-recording-home-energy-consumption-every-15-minutes-search-seventh-circuit-rules [https://perma.cc/2VJG-LK2J] [hereinafter Kerr, *Seventh Circuit Rules*].

[188] *See infra* notes 192–247 and accompanying text.

[189] *See infra* notes 192–218 and accompanying text.

[190] *See infra* notes 219–238 and accompanying text.

[191] *See infra* notes 239–247 and accompanying text.

A. Smart Meter Data

Smart meters are quickly finding their way into homes throughout the United States.[192] Today, smart meters are installed in nearly half of all homes in the United States, and the U.S. Energy Information Administration expects that eighty percent of homes will have smart meters by 2020.[193] Though these numbers seem high, many people already have smart meters in their homes without knowing it.[194] This is because, like traditional meters, homeowners generally do not interact with smart meters.[195] The meters are simply there to "collect, measure, and analyze energy consumption data for grid management, outage notification, and billing purposes."[196]

Smart meters record consumer electricity usage in real time.[197] This data is then transmitted to the utility company.[198] To be useful to the utility company, smart meter data must be granular.[199] As a result, the data can reveal what

---

[192] *See* U.S. Energy Info. Admin., *Nearly Half of All U.S. Electricity Customers Have Smart Meters*, EIA (Dec. 6, 2017), https://www.eia.gov/todayinenergy/detail.php?id=34012 [https://perma.cc/3ZAY-7DBV] (noting that "[i]nstallations of smart meters have more than doubled since 2010").

[193] *Id.* In the United Kingdom, the government aims for every citizen to have a smart meter by 2020, with an option to opt out of installation. GOV.UK, *Smart Meters: A Guide* (Jan. 4, 2018), https://www.gov.uk/guidance/smart-meters-how-they-work [https://perma.cc/X8N8-BXEN]. The UK has adopted the General Data Protection Regulation (GDPR), which provides the "world's strongest data protection rules." Matt Burgess, *What Is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED (Jan. 21, 2019), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 [https://perma.cc/5MT6-3TVK]. In countries that adopt the GDPR, utility companies that offer smart meters must meet the stringent standards set forth by the GDPR. Frost & Sullivan, *Impact of General Data Protection Regulation (GDPR) on Smart Meters and Smart Pumps* (Apr. 4, 2018), https://ww2.frost.com/frost-perspectives/impact-of-general-data-protection-regulation-gdpr-on-smart-meters-and-smart-pumps/ [https://perma.cc/4EA2-UH5V].

[194] U.S. Energy Info. Admin., *supra* note 192. In 2015, only about half of households with a smart meter reported that they either did not have one or did not know if they had one. *Id.*; *see, e.g.*, Sandra Chianfoni et al., *Petition: Halt Massachusetts Smart Meter Program*, CHANGE.ORG, https://www.change.org/p/halt-massachusetts-smart-meter-program [https://perma.cc/PQY9-XN3K] (indicating that utility companies have "installed wireless and smart meters without . . . consent"). Some state legislatures have responded to these privacy concerns by enacting or attempting to enact bills that would allow customers to opt out of smart meter data installation. *See* S. Bill 7214 (N.Y. 2018) (establishing the right to opt out when a utility company seeks to replace a traditional meter with a smart meter and making it illegal for a company to "install any two-way smart meter device . . . without [a] customer's consent").

[195] DEP'T OF ENERGY, COMMUNICATIONS REQUIREMENTS OF SMART GRID TECHNOLOGIES 1 (2010) [hereinafter DEP'T OF ENERGY REPORT]. When smart meters are used in buildings, building managers can monitor the performance of the smart meter in real-time. SIEMENS, SMART ENERGY CONSUMPTION AND THE SMART GRID 3 (2010).

[196] DEP'T OF ENERGY REPORT, *supra* note 195.

[197] *See* CRS SMART METER REPORT, *supra* note 6, at 3 (noting that the collection of data every fifteen seconds results in data being practically recorded in "real-time").

[198] *Id*. Specifically, the data can be transmitted via fiber optic networks, wireless networks, satellite, and power lines. *Id.* at 6.

[199] *Id.* at 1–2.

appliances a consumer is using and at what time.[200] Every appliance in a person's home has an electric load signature that is unique to that appliance.[201] By comparing smart meter data and electric load signatures, it is possible to identify what appliances a person is using at a given time.[202] If this data is aggregated over time, it could reveal a person's daily home life.[203] For example, smart meter data could show that a person is not home every Saturday morning from 9:00 a.m. to 11:00 a.m.[204] It could show that a person typically goes to sleep at 10:00 p.m.[205] It could show that a person cooks dinner three times per week.[206] If a person has visitors for the weekend, smart meter data can show that, too.[207]

The granularity of smart meter data is necessary to realize the benefits of smart meters.[208] Specifically, this data enables smart meters to generate time-based pricing, where a utility company can charge higher prices when there is higher demand for electricity.[209] For example, electricity might cost more at 5:00 p.m. when most people go home after work, but might be cheaper at 3:00

---

[200] NIST SMART GRID REPORT, *supra* note 7, at 10–11. An Italian study identified "heavy-load appliance uses" with ninety percent accuracy using fifteen-minute interval data from a smart meter. ELIAS LEAK QUINN, SMART METERING & PRIVACY: EXISTING LAW AND COMPETING POLICES: A REPORT FOR THE COLORADO PUBLIC UTILITIES COMMISSION 3 n.7 (2008).

[201] NIST SMART GRID REPORT, *supra* note 7, at 10–11. The technique used to determine which appliances are present in the home is referred to as a nonintrusive appliance load monitoring (NALM) technique. *Id.* at 10. NALM techniques have been used to monitor energy demand and usage. *Id.* at 11. This information can be helpful to utility companies who can use the data to increase energy efficiency. *Id.*

[202] CRS SMART METER REPORT, *supra* note 6, at 4.

[203] NIST SMART GRID REPORT, *supra* note 7, at 11. The smart meter itself, however, only measures total energy consumption in fifteen-minute intervals. *Id.* at 9. To identify appliances and usage patterns, the data must be compared against other information. *Id.* at 11.

[204] *See id.* at 28 (noting that "[a]ccess to data-use profiles that can reveal specific times and locations of electricity use in specific areas of the home can also indicate the types of activities and/or appliances used").

[205] *See id.* at 28 n.71 (explaining that smart meter data can reveal that a toaster was used at 8:00 am, 10:00 am, and 12:00 pm).

[206] *See id.* at 34 (providing that "appliance usage data could indicate how often meals are cooked with the microwave, the stove, or not cooked at all, as well as implying the frequency of meals").

[207] *See id.* at 29 (explaining how smart meter data can uncover how many people are in the home).

[208] CRS SMART METER REPORT, *supra* note 6, at 1–2.

[209] SIEMENS, *supra* note 195, at 7. If there was a breach of smart meter data, criminals could find out when homes are unoccupied, or may use the data to stalk victims. McKenna et al., *supra* note 22, at 808. Smart meter data could also be sold to third parties. *See id.* (providing that commercial uses of smart meter data raise privacy concerns). For example, utility companies could sell the smart meter data to Samsung, which might purchase such data and use it to inform a potential customer that their current refrigerator is inefficient and that they should buy a new refrigerator from Samsung. *See id.* (noting that targeted advertising is a privacy concern of smart meter data). Additionally, smart meter data might be used in a custody battle to determine whether a child was left home alone. *Id.* Likewise, a landlord might use smart meter data to determine that there are too many occupants living in a home. *Id.* The data could also be used to monitor a spouse's behavior, such as determining whether one spouse was home alone all week when the other spouse was away. *See id.* (noting that "partners investigating each other's behavior" is a privacy concern resulting from smart meter data).

a.m. when most people are sleeping.[210] The time-stamped data is therefore necessary to alert the utility company to the times when people consume the most electricity.[211] Moreover, smart meters can collect data from a smart grid to monitor these real-time energy prices.[212]

In addition, because of the unreliability of the current electrical grid, the installation of smart meters has become a priority for the national government.[213] Additionally, smart meters can help contribute to a greener environment by reducing the consumption of fossil fuel resources.[214] This is because smart meters can provide detailed feedback to homeowners about their habits to help change consumer behavior and reduce costs.[215] Detailed feedback is also provided to utility companies to allow the company to react quickly in the case of a blackout.[216] Furthermore, utility companies can instruct smart meters to alter a consumer's electricity usage.[217] Lastly, smart meters are often cheaper than traditional meters, which incentivizes the adoption of smart meters for both utility companies and consumers.[218]

---

[210] *See* U.S. Dep't of Energy Office of Elec. Delivery & Energy Reliability, *Time Based Rate Programs*, SMARTGRID.GOV (Mar. 8, 2019), https://www.smartgrid.gov/recovery_act/time_based_rate_programs.html [https://perma.cc/NZM4-JGW8] (discussing several forms of time-based pricing rates: time-of-use pricing, real-time pricing, variable peak pricing, critical peak pricing, and critical peak rebates).

[211] *See id*. (explaining that the frequency of data collection enables time-based pricing).

[212] *Id.*

[213] *See* 42 U.S.C. § 1306 (2018) (authorizing federal funding for smart grid investment); U.S. Dep't of Energy Office of Elec. Delivery & Energy Reliability, *supra* note 210 (noting that the "program is aimed to accelerate the modernization of the nation's electric transmission and distribution systems"); U.S. DEP'T OF ENERGY, AMI REPORT, *supra* note 9, at 4 (noting that the Smart Grid Investment Program tested 16.3 million smart meters); *see also* Brendan Cook et al., *The Smart Meter and a Smarter Consumer: Quantifying the Benefits of Smart Meter Implementation in the United States*, CHEMISTRY CENT. J. 1, 1 (2012) (summarizing the major problems of the current electrical grid resulting from antiquated technology).

[214] SIEMENS, *supra* note 195, at 80. *But see* David O. Carpenter, *Smart Meters: Correcting the Gross Misinformation*, LA MAISON (June 11, 2012), https://maisonsaine.ca/actualites/smart-meters-correcting-the-gross-misinformation.html [https://perma.cc/C85X-VJSW] (finding potential health risks associated with smart meters such as increased cancer rates).

[215] U.S. DEP'T OF ENERGY, AMI REPORT, *supra* note 9, at 28. In 2012, the Oklahoma Gas and Electric Project reported that ninety-nine percent of customers saved money when they installed smart meters. *Id.* at 32. On average, residential customers saved $191.78 per year while commercial customers saved $570.02 per year. *Id. But see* Paul Hyde, *'Shocking' Electricity Bills Spark Concern About Smart Meters in the Upstate, but Duke Says They're Accurate*, GREENVILLE NEWS (Apr. 30, 2018), https://www.greenvilleonline.com/story/news/2018/04/30/shocking-electricity-bills-spark-concern-smart-meters-upstate-but-duke-says-theyre-accurate/554708002/ [https://perma.cc/PD86-889Q] (describing the stories of customers who experienced an increase in electric bills after adopting smart meters).

[216] NIST SMART GRID REPORT, *supra* note 7, at 4.

[217] *Id.*

[218] U.S. DEP'T OF ENERGY, AMI REPORT, *supra* note 9, at 28.

B. Naperville Smart Meter Awareness v. City of Naperville*'s Recognition of Fourth Amendment Rights in Smart Meter Data*

Prior to the Seventh Circuit's ruling in *Naperville*, there was practically no guidance by courts on the Fourth Amendment consequences of the collection of smart meter data.[219] The City of Naperville received funds from the U.S. Department of Energy to update the city's electrical grid.[220] This non-investigatory use of smart meter data by the government implicated the Fourth Amendment.[221] The smart meter installation in Naperville was mandatory; residents could not opt out.[222] Naperville Smart Meter Awareness, a group of concerned citizens, sued Naperville alleging Fourth Amendment violations.[223]

The Seventh Circuit found that the smart meter data collected at fifteen-minute intervals was a search.[224] The court compared smart meter data to the thermal images in *Kyllo* and found that smart meters were much more intru-

---

[219] *See* CRS SMART METER REPORT, *supra* note 6, at 8 (noting that "there is no Fourth Amendment case on point"). *See generally* Balough, *supra* note 5, at 160, 183–85 (discussing the Fourth Amendment's application to smart meters); Duarte, *supra* note 5, at 1153–56 (analyzing the Fourth Amendment's applicability to smart meters). *But see* Detroit Edison Co. v. Stenman, 875 N.W.2d 767, 778 (Mich. Ct. App. 2015) (holding that there was no government action that would implicate the Fourth Amendment when smart meters were placed without consent by a privately-owned electric utility).

[220] *Naperville*, 900 F.3d at 524. Under the American Recovery and Reinvestment Act of 2009, the Department of Energy must allocate funds to different cities across the nation in exchange for installing smart meters. 42 U.S.C. § 1306 (2018); *Naperville*, 900 F.3d at 524.

[221] *See Naperville*, 900 F.3d at 529 (noting that the public utility did not have an investigatory purpose in collecting the data); United States v. Attson, 900 F.2d 1427, 1430 (9th Cir. 1990) (noting that the Supreme Court rarely hears cases about the Fourth Amendment in the situation where there is "noncriminal non-investigatory governmental conduct").

[222] *Naperville*, 900 F.3d at 524. This is unlike other cities, which have allowed residents to opt-out of the program. *See, e.g.*, Vickie Aldous, *Opting Out of 'Smart Meters' Could Cost Ashland Residents*, MAIL TRIB. (June 9, 2012), https://mailtribune.com/archive/opting-out-of-smart-meters-could-cost-ashland-residents [https://perma.cc/JXP7-VESK] (discussing the expenses associated with one city's opt-out); Christian Hill, *After Public Input, Oregon Utility Offers Smart Meter Opt-Out Policy*, GOV'T TECH. (Feb. 8, 2018), http://www.govtech.com/data/After-Public-Input-Oregon-Utility-Offers-Smart-Meter-Opt-Out-Policy.html [https://perma.cc/H4P8-AQ2N] (explaining Oregon's smart meter opt-out policy).

[223] *Naperville*, 900 F.3d at 524. The citizens also alleged a violation of a similar provision in the Illinois Constitution. *Id.* Initially, the citizens argued that the fact that they were unable to retain their analog meters was a violation of their equal protection rights. *Naperville I*, 69 F. Supp. 3d at 842. The U.S. District Court for the Northern District of Illinois, however, granted summary judgment to the city because the citizens were unable to prove that the city allowed some citizens to keep their analog meters but not others. *Id.*

[224] *Naperville*, 900 F.3d at 529. Similar to *Carpenter*, the Seventh Circuit cautioned that the holding was narrowly limited to data collected at fifteen-minute intervals. *Id.*; *see* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (explicitly noting that the holding was limited to seven days of cell-site location information). If the data was collected at intervals shorter than fifteen minutes or made more accessible to parties outside the utility, the court noted that their "conclusion could change." *Naperville*, 900 F.3d at 529.

sive.[225] Compared to *Kyllo*, where the technology revealed that something was emitting a large amount of energy, smart meter data can reveal "when people are home, when people are away, when people sleep and eat, what types of appliances are in the home, and when those appliances are used."[226] Additionally, the court reasoned that the inference made in *Kyllo*, that high energy readings correlate to growing marijuana, could easily be made by smart meter data.[227]

The Seventh Circuit noted that a search does not occur when technology is "widely available and routinely used by the public," as set forth in *Kyllo*.[228] Without more, the court noted that the meters "have been adopted only by a portion of a highly specialized industry."[229] Therefore, the court found that the "general public use" exception did not apply to smart meters.[230] Although the Seventh Circuit found that smart meter data collection was a search, the court found that the search was reasonable.[231] Because there was no law enforcement action, the court used a reasonableness balancing inquiry rather than the traditional probable cause inquiry used for warrants.[232] To determine reasonableness, the court weighed a person's privacy interests in smart meter data against the legitimate government interest in collecting that data.[233] Even though the court recognized that individuals have a privacy interest in their

---

[225] *Naperville*, 900 F.3d at 526.

[226] *Id.*

[227] *Id.* Moreover, the court noted that, by using NALM techniques to correlate a grow light's energy consumption signature and the energy consumption pattern of a home, the inference is even stronger than that in *Kyllo*. *Id.*; *see* Kyllo v. United States, 533 U.S. 27, 29 (2001) (describing a law enforcement agent's use of a high thermal energy reading to support the fact a person was growing marijuana in his home). *But see* United States v. McIntyre, 646 F.3d 1107, 1111 (8th Cir. 2011) (rejecting the proposition that just because the same inference was made in *Kyllo*, high energy meter readings do not warrant Fourth Amendment protection because there is a difference between physically using a thermal imaging device and asking a third-party for energy records).

[228] *Naperville*, 900 F.3d at 527; *see Kyllo*, 533 U.S. at 40 (indicating that the use of a technology is not a search when the technology is generally used by the public).

[229] *Naperville*, 900 F.3d at 527. This part of the decision has been widely criticized because the Seventh Circuit does not point to any facts regarding how many people have smart meters. Bernard Bell, *Too Smart by Half:* Naperville Smart Meter Awareness v. City of Naperville, YALE J. REG.: NOTICE & COMMENT BLOG (Nov. 6, 2018), http://yalejreg.com/nc/too-smart-by-half-naperville-smart-meter-awareness-v-city-of-naperville/ [https://perma.cc/TD98-RW99]. Instead, the court seems to rely more on "judicial intuition." Kerr, *Seventh Circuit Rules*, *supra* note 187.

[230] *Naperville*, 900 F.3d at 527.

[231] *Id.* The general presumption is that a warrantless search is unreasonable. *Kyllo*, 533 U.S. at 42.

[232] *Naperville*, 900 F.3d at 528. The court also discussed the administrative search doctrine. *Id.* The administrative search doctrine recognizes that the government conducts searches without requiring probable cause. Eve B. Primus, *Bringing Clarity to Administrative Search Doctrine: Distinguishing Dragnets from Special Subpopulation Searches*, 39 SEARCH & SEIZURE L. REP. 61, 62 (2012). For example, administrative searches are those typically done at an airport or at public schools. *Id.* at 61. To determine whether an administrative search is reasonable, a court must weigh the government's interest in carrying out the search and the invasion of a person's privacy. *Id.* Accordingly, an administrative search does not require a heightened showing of probable cause. *Id.* at 62.

[233] *Naperville*, 900 F.3d at 528.

energy consumption data, the court found the collection of smart meter data to be much less intrusive than typical Fourth Amendment searches.[234]

Holding that the search was reasonable, the Seventh Circuit emphasized that the search was not associated with law enforcement and thus presented no risk of criminal consequences for individuals.[235] In addition, the court found that Naperville's "Smart Grid Customer Bill of Rights," which clarifies that the public utility will not provide customer data to third parties, was a sufficient safeguard against further dissemination of smart meter data.[236] Ultimately, the strong government interest in smart meters and the benefits of such meters outweighed the citizen's privacy interests.[237] Importantly, because *Naperville* did not involve law enforcement access to the data, the court did not apply the third-party doctrine.[238]

C. The Third-Party Doctrine

The City of Naperville argued that, under the third-party doctrine, citizens have no reasonable expectation of privacy in smart meter data.[239] Specifically, the City argued that citizens give up their expectation of privacy in energy data when they purchase electricity from the City.[240] The Seventh Circuit, however, refused to apply the third-party doctrine because there was no third party: the data flowed directly from the citizen to the government in the form of a public utility.[241] The court found that even if a public utility could be considered a

---

[234] *Id.*

[235] *Id.* The court mentioned the fact that a public utility does not have prosecutorial intent when collecting and reviewing the data. *Id.* The court relied on the Supreme Court's decision in 1967 in *Camara v. Municipal Court of San Francisco*. *Id.* In *Camara*, building inspectors conducted a search under the Fourth Amendment when they entered the defendant's building. 387 U.S. 523, 526 (1967). There, the Court emphasized the fact that by refusing entry to the building inspector, the defendant could be prosecuted under a state law that made it a crime to refuse to comply with building inspectors' requests. *Id.* at 537–38. Ultimately, the *Naperville* court followed *Camara* in holding that a lack of prosecutorial intent lessens an individual's privacy interest. *See Naperville*, 900 F.3d at 527 (noting that the "[r]isk of corollary prosecution that troubled the court in *Camara* is minimal here").

[236] *Naperville*, 900 F.3d at 528.

[237] *Id.* at 528–29. The court noted several benefits of smart meters. *Id.* Specifically, smart meters allow utilities to restore power quickly, time-based pricing results in cost savings, and smart meters encourage energy efficiency. *Id.*

[238] *See infra* notes 239–246 and accompanying text.

[239] *Naperville*, 900 F.3d at 527. The third-party doctrine typically applies to business records. *See e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (phone records); United States v. Miller, 425 U.S. 435, 443 (1976) (bank records); Couch v. United States, 409 U.S. 322, 340 (1973) (tax documents).

[240] *Naperville*, 900 F.3d at 527. Interestingly, the Northern District of Illinois applied the third-party doctrine to smart meter data and found that Naperville citizens consented to the collection of their data. *See Naperville I*, 69 F. Supp. 3d at 840 (finding that the public utility could be considered a third-party for Fourth Amendment purposes).

[241] *Naperville*, 900 F.3d at 527. According to one scholar, the court seemed to think that not applying the third-party doctrine was in favor of the defendants. *See* Kerr, *Seventh Circuit Rules*, *supra*

third party, *Carpenter* indicated that the doctrine would not apply in this case.[242] Specifically, the court reasoned that because the Naperville citizens could not opt out of smart meter installation, they did not "voluntarily" share information with the public utility.[243] Additionally, the court reasoned:

> If a person does not—in any meaningful sense—"voluntarily 'assume the risk' of turning over a comprehensive dossier of physical movements" by choosing to use a cell phone, it also goes that a home occupant does not assume the risk of near constant monitoring by choosing to have electricity in her home.[244]

Seemingly, the Seventh Circuit followed *Carpenter* in examining how voluntary an action must be to trigger the third-party doctrine.[245] The court noted, however, that if the City gave Naperville citizens a choice to opt out of smart meter installation, "Naperville could have avoided this controversy."[246] The court did not address, however, whether a person who opts-in to smart meter installation, perhaps to save money, would be considered to have given up their Fourth Amendment rights in the data if the third-party doctrine applied.[247]

---

note 187. The court failed to consider the fact that the third-party doctrine evolved from cases where disclosures were made directly to the government. *Id.*; *see, e.g.*, United States v. White, 401 U.S. 745, 750 (1971) (involving a confession of crimes to a friend wearing a wire); Hoffa v. United States, 385 U.S. 293, 295 (1966) (regarding a person's incriminating statements to a co-worker who was an undercover informant); Lewis v. United States, 385 U.S. 206, 210 (1966) (concerning a sale of marijuana to an undercover agent); Lopez v. United States, 373 U.S. 427, 435 (1963) (involving an attempt to bribe an IRS agent); Lee v. United States, 343 U.S. 747, 758 (1952) (holding that the Fourth Amendment did not protect a person who made incriminating statements to a friend secretly working with the police).

[242] *Naperville*, 900 F.3d at 527. Some commentators have suggested that in cases where law enforcement is involved, *Carpenter* does not apply because there would still be no third party. Bell, *supra* note 229; *see* Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 51 (1995) (noting that "if the state can obtain the information only through means constituting a search or seizure, then use restrictions should apply, confining the governmental authorities to uses consistent with the Amendment's reasonableness requirement"). For example, because the "government," or the public utility, has already collected the data, the legal landscape changes because the Fourth Amendment is not considered with the further sharing of information obtained by an initial search. *Id.*; Bell, *supra* note 229.

[243] *Naperville*, 900 F.3d at 527.

[244] *Id.* (quoting *Carpenter*, 138 S. Ct. at 2220).

[245] *Id.* (noting that the action at issue in *Carpenter*—sharing location information with a phone company—is not "voluntary").

[246] *Id.* at 529. The court rejected the argument that Naperville citizens engaged in a "voluntary relationship" with the public utility to purchase electricity. *Id.* at 527.

[247] *Cf. id.* at 527.

IV. SMART METER DATA SHOULD BE PROTECTED BY THE FOURTH AMENDMENT

The Fourth Amendment protects against unreasonable searches.[248] Whether a search has occurred depends, in part, on whether there is an expectation of privacy that society recognizes as reasonable.[249] Due to the granularity and wide latitude of information inferred from smart meter data, law enforcement agents will likely attempt to access such data soon.[250] This is because smart meter data has the potential to alert law enforcement to a wide-range of illicit behavior.[251] Moreover, the data bears strong similarities to the searches in *Kyllo* and *Carpenter*.[252] As a result, the Fourth Amendment should be applicable to smart meter data.[253] Section A of this Part explains why an individual's reasonable expectation of privacy in the home supports the application of the Fourth Amendment to smart meter data.[254] Section B illustrates why the third-party doctrine does not apply to smart meter data.[255] Section C clarifies the motivation behind requiring law enforcement to obtain a warrant to access smart meter data.[256]

A. A Person Has a Reasonable Expectation of Privacy in Smart Meter Data

The Supreme Court has consistently emphasized that, as far as the Fourth Amendment is concerned, the home is "first among equals."[257] Because smart

---

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

[249] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). To trigger the Fourth Amendment there must be government action. *See* United States v. Knights, 534 U.S. 112, 118 (2001) (emphasizing that "the touchstone of the Fourth Amendment is reasonableness"); Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (holding that an illegal search conducted by private persons did not implicate the Fourth Amendment).

[250] NIST SMART GRID REPORT, *supra* note 7, at 11. The data will likely be sought for purposes that go beyond investigations into marijuana production. *See* United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1117 (9th Cir. 2012) (utilizing energy consumption records in a marijuana investigation); United States v. Hoang, 487 F. App'x 239, 245 (6th Cir. 2012) (utility records supported probable cause for the search of defendant's home); United States v. McIntyre, 646 F.3d 1107, 1111 (8th Cir. 2011) (involving the use of electric records in a marijuana investigation); McKenna et al., *supra* note 22, at 808 (noting that law enforcement agencies could use smart meter data to detect a variety of illegal activities occurring in a person's home).

[251] Lerner & Mulligan, *supra* note 119, at 6.

[252] *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (involving a large quantity of cell-site location information that was aggregated to reveal a person's behavior); Kyllo v. United States, 533 U.S. 27, 40 (2001) (involving a search of the home utilizing thermal imaging technology).

[253] *See* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 529 (7th Cir. 2018) (affording smart meter data Fourth Amendment protections when a public utility collects the data and citizens cannot opt-out).

[254] *See infra* notes 257–288 and accompanying text.

[255] *See infra* notes 289–304 and accompanying text.

[256] *See infra* notes 305–318 and accompanying text.

[257] Florida v. Jardines, 569 U.S. 1, 6 (2013); *see* California v. Ciraolo, 476 U.S. 207, 213 (1986) (finding that "privacy expectations are most heightened" in the context of the home); Oliver v. United

meters have the potential to reveal vast amounts of information about people's habits in their homes, the resulting data is deserving of Fourth Amendment protection.[258] In *Kyllo*, a federal agent used a thermal image scan to discern that the defendant had something in his home emitting an abnormally high amount of heat energy.[259] There, the Supreme Court held that the thermal image scan was a search.[260] Similarly, a law enforcement agent could use smart meter data to determine that a person is growing marijuana due to abnormally high energy consumption.[261] Though this inference has been supported by traditional energy records obtained via a subpoena, smart meter data goes a step further because it can precisely reveal that a person owns a marijuana grow light.[262]

Moreover, smart meter data is sense-enhancing, as was the technology in *Kyllo*.[263] It allows police to gain information otherwise unavailable without physical entry.[264] But smart meters have the potential to reveal significantly more information about what goes on inside a home than the thermal imaging device in *Kyllo*.[265] For example, smart meter data could reveal a surge of energy coming from a microwave at a particular time, which might be useful in a case where a microwave was being used as a murder weapon.[266] Certainly, it

---

States, 466 U.S. 170, 180 (1984) (extending the Fourth Amendment to areas "immediately surrounding and associated with the home"); Silverman v. United States, 365 U.S. 505, 511 (1961) (noting that "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").

[258] *See* U.S. DEP'T OF ENERGY, SMART GRID REPORT, *supra* note 12, at 2 (providing that smart meters can uncover the times people are in their homes, when occupants shower, the types of appliances in the home and when they are used); *see also* CRS SMART METER REPORT, *supra* note 6, at 4 (describing several incriminating inferences resulting from smart meter data).

[259] *Kyllo*, 533 U.S at 29.

[260] *Id.* at 38.

[261] *Naperville*, 900 F.3d at 526; *see Kyllo*, 533 U.S at 30 (noting that the FBI used high thermal energy records to obtain a warrant to search the defendant's home based on suspicion that the defendant was growing marijuana).

[262] *See Naperville*, 900 F.3d at 526 (finding that smart meter data can be used to conclude that a person owns marijuana grow lights); United States v. McIntyre, 646 F.3d 1107, 1111 (8th Cir. 2011) (involving the use of electric records in a marijuana investigation).

[263] *Compare* Kerr, *The Fourth Amendment and New Technologies*, *supra* note 30, at 801 (arguing that "courts should place a thumb on the scale in favor of judicial caution when technology is in flux, and should consider allowing legislatures to provide the primary rules governing law enforcement investigations involving new technologies"), *with* Daniel J. Solove, *The Coexistence of Privacy and Security: Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 747 (2005) (criticizing Orin Kerr's approach and demonstrating that legislative rules are deficient when compared to the Fourth Amendment).

[264] *See* U.S. DEP'T OF ENERGY, SMART GRID REPORT, *supra* note 12, at 2 (explaining how smart meter data can lead to information about what a person is doing in their home).

[265] CRS SMART METER REPORT, *supra* note 6, at 19; *see Naperville*, 900 F.3d at 526 (comparing smart meter data to the thermal imaging device used in *Kyllo*).

[266] *See* NIST SMART GRID REPORT, *supra* note 7, at 34 (noting that smart meter data can reveal when a microwave is in use); Mike Riggs, *The Microwave as a Murder Weapon: A Brief History*, CITYLAB (Mar. 13, 2014), https://www.citylab.com/life/2014/03/microwave-murder-weapon-brief-

would be difficult for police to learn this information without entering a person's home at that time.[267]

In *Carpenter*, the FBI used hundreds of cell-site location data points to conclude that the suspect was in the vicinity of the robberies at the time they took place.[268] Like CSLI, smart meter data is time-stamped; it can reveal what a person is doing in their home at a particular time.[269] This allows law enforcement agents to "travel back in time," limited only by how long the utility company retains the data.[270] It is hard to imagine a more "intimate window into a person's life" than discerning whether a person is home, away, asleep, awake, eating, doing laundry, watching television, or listening to music at a certain time.[271] Moreover, like *Carpenter*, these data points are collected within seconds.[272] By amassing this type of data over, for example four months, law enforcement could re-create a person's home life down to every fifteen seconds over those four months.[273]

In 2018, the Seventh Circuit held in *Naperville* that citizens have Fourth Amendment rights in the collection of their smart meter data.[274] The court, however, left a fracture in their Fourth Amendment analysis.[275] Specifically, the Seventh Circuit found that smart meters are not yet in general public use, so it would be unfair for the government to collect this data without deeming it a search.[276] The court relied on *Kyllo*, where the Supreme Court found the fact that thermal-imaging devices were not yet in general public use to be significant in holding that the search of the home violated the Fourth Amendment.[277]

---

history/8626/ [https://perma.cc/7WJJ-MN5V] (discussing microwaves being used as murder weapons).

[267] *See* Riggs, *supra* note 266 (describing some of the challenges associated with investigation of crimes where a microwave was being used as a murder weapon).

[268] *Carpenter*, 138 S. Ct. at 2221.

[269] *See* NIST SMART GRID REPORT, *supra* note 7, at 31.

[270] *Carpenter*, 138 S. Ct. at 2218; *see* NIST SMART GRID REPORT, *supra* note 7, at 55 (proposing that smart meter data "should be retained only for as long as necessary to fulfill the purposes that have been communicated to energy consumers").

[271] *Carpenter*, 138 S. Ct. at 2217; *see* CRS SMART METER REPORT, *supra* note 6, at 4 (describing the inferences that smart meter data can make).

[272] *See Carpenter*, 138 S. Ct. at 2217 (noting that cell-site location information is "detailed, encyclopedic, and effortlessly compiled"); CRS SMART METER REPORT, *supra* note 6, at 4 (providing that smart meter data is collected every fifteen seconds); Bloom & Clark, *supra* note 61, at 197 (describing the science behind cell-site location information and emphasizing that a cell phone can ping to a cell tower every few seconds).

[273] *See Carpenter*, 138 S. Ct. at 2217 (noting that "mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts").

[274] *Naperville*, 900 F.3d at 527.

[275] *See* Kerr, *Seventh Circuit Rules*, supra note 187 (criticizing the *Naperville* decision).

[276] *Naperville*, 900 F.3d at 527.

[277] *Id.*; *see Kyllo*, 533 U.S at 34 (explaining the "general public use" exception). The "general public use" doctrine appears to sanction the reduced Fourth Amendment protections when the relevant technology is widely used. *Kyllo*, 533 U.S. at 46–47 (Stevens, J., dissenting); *see* Adkins, *supra* note

There, the Supreme Court implied that once a technology is in general public use then Fourth Amendment protections will disappear.[278] It is unclear what the standard for general public use is, but according to current statistics, smart meters are used in a majority of American homes.[279] The "general public use" exception thus has the potential to undermine and threaten the Fourth Amendment protections that smart meter data should be afforded.[280]

Instead, the Seventh Circuit should have distinguished the general public use exception in *Kyllo* and *Naperville* by inquiring into the purpose of the new technology.[281] In *Kyllo*, police used the technology for the sole purpose of investigation.[282] In contrast, utility companies use smart meters like traditional meters, to collect energy readings.[283] These divergent purposes should be legally significant if the policy behind the general public use exception is given any weight.[284] The general public use exception is premised on the notion that police should not use technology-assisted devices that the general public does not have access to in order to bypass the Fourth Amendment.[285] This policy is not as sound when it comes to smart meter data because the data is being created regardless of an investigative purpose; the data is not being created at the

---

55, at 252–67 (explaining the subjectivity involved in any application of the "general public use" doctrine).

[278] *Kyllo*, 533 U.S at 46–47 (Stevens, J., dissenting).

[279] *See* Adkins, *supra* note 55, at 245 (explaining the lack of Supreme Court guidance on the "general public use" doctrine); CRS SMART METER REPORT, *supra* note 6, at 18 (describing the uncertainty regarding the "general public use" doctrine's applicability to smart meter data); U.S. Energy Info. Admin., *supra* note 192 (noting that approximately fifty percent of U.S. customers have smart meter data). *Compare* United States v. Vela, 486 F. Supp. 2d 587, 590 (W.D. Tex. 2005) (finding vision goggles used by the military to be in general public use because one could purchase the goggles online), *with* United States v. Dellas, 355 F. Supp. 2d 1095, 1107 (N.D. Cal. 2005) (denying Fourth Amendment protection to vision goggles).

[280] Adkins, *supra* note 55, at 245; *see* Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1400–08 (2002) (exploring what it means for something to be in general public use); S. Alex Spelman, *Drones: Updating the Fourth Amendment and the Technological Trespass Doctrine*, 16 NEV. L.J. 373, 378 (2015) (arguing that the "general public use doctrine" wrongly denies Fourth Amendment protections to popular technologies, such as drones).

[281] *See Kyllo*, 533 U.S at 29 (describing the FBI's use of the thermal imaging device to scan the defendant's home).

[282] *Id.*

[283] *See* CRS SMART METER REPORT, *supra* note 6, at 5 (explaining how frequent data collection helps utility companies identify electricity demand and set electric prices). Yet courts should treat smart meters differently than traditional meters because they have the potential to reveal much more information. *See* NIST SMART GRID REPORT, *supra* note 7, at 9 (describing the differences between smart meter data and traditional energy data and explaining the inferences made from smart meter data).

[284] *See infra* notes 285–288 and accompanying text.

[285] *See Kyllo*, 533 U.S at 34–35 (discussing the significance of the fact that the thermal imaging device was not in general public use and the impact it has on an individual's reasonable expectation of privacy).

direction of law enforcement agents.[286] In sum, smart meters have an independent purpose, whereas the thermal imaging device in *Kyllo* was used solely for investigative purposes.[287] Although the Seventh Circuit found that the general public use exception does not apply because smart meters are not generally used, the court nonetheless sanctioned future courts to remove Fourth Amendment protections after a court finds that a majority of American homes have smart meters.[288]

B. The Third-Party Doctrine Should Not Apply to Smart Meter Data

In 2018, the Seventh Circuit in *Naperville* held that the third-party doctrine did not apply because no third party was involved; the smart meter data flowed directly from the individual to the government.[289] In cases where law enforcement is involved, however, one can assume that there are three parties: the individual, the utility, and law enforcement.[290] Nonetheless, in the case where law enforcement seeks access to smart meter data, the third-party doctrine should not apply.[291]

Individuals likely do not assume the risk of releasing data to law enforcement when they own a smart meter, or at least do not assume the risk of releasing the inferences drawn therefrom.[292] In other words, even if a person

---

[286] *See* CRS SMART METER REPORT, *supra* note 6, at 2 (explaining the history behind smart meters as a means to combat challenges resulting from the need to modernize the electrical grid).

[287] *Compare Kyllo*, 533 U.S at 29 (describing the FBI's use of the thermal imaging device to scan the defendant's home for evidence connecting the suspect to marijuana production), *with* NIST SMART GRID REPORT, *supra* note 7, at 29 (describing non-investigatory purposes of smart meters to increase energy efficiency and reduce costs for utilities and consumers).

[288] *See Naperville*, 900 F.3d at 526–27 (finding that smart meters are not yet in general public use).

[289] *Id.* at 525.

[290] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (involving an individual, a phone company, and law enforcement); United States v. Miller, 425 U.S. 435, 443 (1976) (involving an individual, a bank, and law enforcement); Couch v. United States, 409 U.S. 322, 340 (1973) (involving an individual, an accountant, and law enforcement); *McIntyre*, 646 F.3d at 1111 (applying the third-party doctrine to traditional energy data, holding that a person does not have a reasonable expectation of privacy in such data). In the case of a public utility, however, the rationale behind the third-party doctrine might still apply. *See* Kerr, *Seventh Circuit Rules*, *supra* note 187 (opining that voluntarily sharing data directly to a public utility is more on par with the "secret agent" cases that recognize that a person does not have a reasonable expectation of privacy in information voluntarily shared with the government).

[291] *See* Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 3 (2013) (arguing that the third party doctrine should not apply to internet records); Alexander Porter, Note, *"Time Works Changes": Modernizing Fourth Amendment Law to Protect Cell Site Location Information*, 57 B.C.L. REV. 1781, 1789 (2016) (arguing that the third party doctrine should not be applied to cell-site location information).

[292] *Naperville*, 900 F.3d at 526–27; *see* Bloom & Clark, *supra* note 61, at 197 (arguing that a person does not voluntarily convey cell-site location information to phone companies because there is no affirmative action). Owning a cell phone is almost a prerequisite for participating in society. Bloom & Clark, *supra* note 61, at 198; *see* People v. Chapman, 679 P.2d 62, 67 (Cal. 1984) (noting that

understands that a utility is collecting their energy meter readings, it is unlikely that anyone meaningfully consents to the inferences drawn therefrom.[293] In *Naperville*, the court indicated that if citizens could opt out of smart meter installation, the third-party doctrine might apply.[294] Nonetheless, courts should look not at whether an individual chose to engage in the behavior in question, but whether the person could reasonably expect that the inferences made from the data would be shared with law enforcement.[295] Indeed, the underlying rationale of the third-party doctrine is that the Fourth Amendment does not protect voluntary disclosures.[296]

In *Carpenter*, the Supreme Court recognized that by making the affirmative decision to own a cellphone, people did not realize that they were allowing the government to access "an exhaustive chronicle of location information."[297] Law enforcement values CSLI because of the inferences it can provide.[298] Thus, *Carpenter* stands for the proposition that the Fourth Amendment should protect individuals when these inferences do not give rise to a reasonable expectation of privacy.[299] The Supreme Court emphasized this idea, even though most individuals would likely not be surprised to learn that their phone was tracking their location.[300] In the case of smart meter data, however, people would be surprised to know that their energy meter data could reveal what time they wake up and go to sleep.[301] Therefore, it is not accurate to say that individuals "voluntarily" share their smart meter data with the utility company.[302]

"[d]oing without a telephone is not a realistic option for most people"); People v. Sporleder, 666 P.2d 135, 141 (Colo. 1983) ("A telephone is a necessary component of modern life. It is a personal and business necessity indispensable to one's ability to effectively communicate in today's complex society."). By merely owning a phone a person does not voluntarily convey their location to their phone company. Bloom & Clark, *supra* note 61, at 198. Similarly, by choosing to have electricity, which doing without "is not a realistic option for most people," a person does not voluntarily convey their activities in the home to their energy utility company. *Chapman*, 679 P.2d at 67; *see* Bloom & Clark, *supra* note 61, at 197–98 (discussing the third-party doctrine's applicability to cell-site location information).

[293] *Naperville*, 900 F.3d at 526–27.

[294] *Id.* at 524.

[295] *See id.* (emphasizing the highly personal nature of the inferences made from smart meter data).

[296] *Smith*, 442 U.S at 743–44; *Miller*, 425 U.S. at 443.

[297] *Carpenter*, 138 S. Ct. at 2219; *cf. Smith*, 442 U.S at 745 (holding that individuals do not expect their phone records to remain private).

[298] *See Carpenter*, 138 S. Ct. at 2220 (explaining that law enforcement agents aimed to use the CSLI to place the suspect at the scene of the crime).

[299] *See id.* (holding that a person has a reasonable expectation of privacy in physical movements).

[300] *See id.*

[301] *See* CRS SMART METER REPORT, *supra* note 6, at 22 (noting that "[e]ven if customers are aware their utility usage can be recorded in sub-fifteen-minute intervals, a reasonable customer would probably be surprised, if not shocked, to know that data from smart meters can potentially be used to pinpoint the usage of specific appliances").

[302] *See* Bloom & Clark, *supra* note 61, at 192 (emphasizing that the third-party doctrine should not apply to cell-site information because it is "generated without the user's knowledge and often without any accompanying affirmative act").

The reasoning of *Naperville* inappropriately enables the application of the third-party doctrine to cases where citizens have a genuine opportunity to consent to smart meter data.[303] Smart meters offer tremendous benefits for consumers over traditional meters.[304] If citizens make the conscious choice to adopt a smart meter in their home instead of a traditional meter, the third-party doctrine still should not apply.[305] This is because a person does not voluntarily share the inferences made from smart meter data in any "meaningful sense."[306]

C. The Need for a Warrant: Compelling a Third Party to Turn Over Data Instead of Law Enforcement Seeking It Directly Is Not a Legally Significant Difference

Recognizing a person's Fourth Amendment rights in smart meter data, the best way to ensure that those rights are protected is to follow *Carpenter* and apply the warrant requirement.[307] In 2011, the Eighth Circuit in *United States v. McIntyre*, held that there was a minimal intrusion on a person's privacy when a subpoena was used to compel records.[308] Justice Alito also takes this position in his dissent in *Carpenter*.[309] In Justice Alito's view, the legal standard should be considered together with whether there is a reasonable expectation of privacy.[310] Thus, documents that are compelled via a subpoena or other administrative process, do not intrude on a person's privacy in a way that has been typically recognized by the Fourth Amendment.[311]

---

[303] *See Naperville*, 900 F.3d at 529 (noting that the city "could have avoided this controversy" if citizens could opt-out of smart meter installation and finding that smart meters were applying the "general public use" doctrine).

[304] *See id.* (performing a balancing test and concluding that the government has a strong interest in smart meters due to the cost-saving benefits); U.S. DEP'T OF ENERGY, AMI REPORT, *supra* note 9, at 12 (reporting the cost-saving results during a test of 16.3 million smart meters); SIEMENS, *supra* note 195, at 3 (explaining the possible reduction of electric demand due to smart meters); U.S. Dep't of Energy Office of Elec. Delivery & Energy Reliability, *supra* note 210 (discussing several benefits of smart meters, such as time-based pricing).

[305] *See* Bloom & Clark, *supra* note 61, at 196–98 (offering support for the proposition that the third-party doctrine should focus on voluntariness).

[306] *See Carpenter*, 138 S. Ct. at 2220 (holding that a person does not "meaningful[ly]" share their location data with their phone company).

[307] *See id.* (requiring a warrant to access seven days of cell-site location information); *supra* notes 257–304 and accompanying text (arguing that the Fourth Amendment protects smart meter data).

[308] *McIntyre*, 646 F.3d at 1111. Similarly, in 2006, the United States District Court for the District of Oregon in *United States v. Hamilton* found that it was "legally significant" that power records were obtained via a subpoena, rather than by intruding on the home by thermal-imaging technology used in *Kyllo*. United States v. Hamilton, 434 F. Supp. 2d 974, 980 (D. Or. 2006).

[309] *Carpenter*, 138 S. Ct. at 2250–57 (Alito, J., dissenting).

[310] *Id.*

[311] *Id.*

Rejecting this argument, the majority in *Carpenter* is sympathetic to what privacy means in a digital age.[312] How law enforcement is collecting data is becoming less important.[313] Though illegal searches are generally thought to occur in a situation where police barge into a person's home, technology is enabling police to gain access to everything they could by walking into the home, without entering.[314] After *Carpenter*, if the government wants to collect CSLI or other records in which a person has Fourth Amendment rights, the government must use a warrant regardless of whether the data is stored at home or remotely.[315] In the "rare case" of smart meter data, requiring law enforcement to obtain a warrant is the only way to protect a person's Fourth Amendment rights.[316] One scholar has even argued that there should be a stricter standard beyond a warrant's probable cause requirement because smart meter data is so personal.[317] If a subpoena could be used to obtain smart meter data, there would be virtually limitless government collection of personal data.[318] The reasonableness standard for a subpoena is too low of a standard to satisfy in order to protect people from unwanted government intrusion.[319] Ultimately,

---

[312] *See id.* at 2214 (majority opinion) (emphasizing that the Supreme Court has adjusted the Fourth Amendment framework where necessary to keep up with technologies and to preserve expectations of privacy).

[313] *See id.* at 2222 (holding that accessing cell-site data from a third party warrants an application of the Fourth Amendment).

[314] *See, e.g.*, *Kyllo*, 533 U.S. at 40 (holding a thermal imaging device allowed law enforcement agents to see inside the home, when they otherwise would not be able to). In the case of smart meter data, law enforcement could likely learn even more information than they could by entering a home. *See* NIST SMART GRID REPORT, *supra* note 7, at 32 n.81 (discussing the various inferences smart meter data can reveal, including the fact that a person lost their job because they were spending large amounts of time at home). Thus, although *Carpenter*'s holding may have signaled a drastic change because it blurred the lines between compelling records and taking them, the holding was necessary if the Fourth Amendment is designed to protect reasonable expectations of privacy. *See* Bloom & Clark, *supra* note 61, at 196 (arguing that cell-site location information deserves Fourth Amendment protection).

[315] *See Carpenter*, 138 S. Ct. at 2222 (holding that "a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party").

[316] *See id.* (holding that law enforcement needs to meet the probable cause standard before accessing data held by a third party in which a subject has Fourth Amendment rights).

[317] *See* Bell, *supra* note 229 (positing that "perhaps the quantum of evidence required should be a bit higher given the granularity of the information such smart meters can provide regarding a person's activities inside their home, a location entitled to the highest privacy protections"). Some have argued that states will do a better job at protecting smart meter data than the Fourth Amendment. Balough, *supra* note 5, at 160, 183–85; Duarte, *supra* note 5, at 1154.

[318] *See Carpenter*, 138 S. Ct. at 2222 (noting that "[i]f the choice to proceed by subpoena provided a categorical limitation on Fourth Amendment protection, no type of record would ever be protected by the warrant requirement . . . . [A]ny personal information reduced to document form, [could] be collected by subpoena for no reason other than 'official curiosity'"). Warrantless searches "are per se unreasonable under the Fourth Amendment." *Katz*, 389 U.S. at 357.

[319] *See Carpenter*, 138 S. Ct. at 2222 (recognizing that, to satisfy the Fourth Amendment, a warrant is required to access information in which a person has Fourth Amendment rights).

the probable cause requirement to obtain a warrant is the only way to protect a person's Fourth Amendment rights in smart meter data.[320]

CONCLUSION

Smart meters, and the technology that enables them, present novel issues regarding the applicability of the Fourth Amendment. At first glance, it may appear as though a traditional Fourth Amendment framework is sufficient to address these issues. As this Note has argued, however, applying that framework would lead to decreased protections for individuals in their homes, an area traditionally given substantial constitutional protections. As the Supreme Court highlighted in *Carpenter*, courts should consider the potential impact of new technologies on personal privacy when determining how to treat such technologies under the Fourth Amendment. Ultimately, the rich detail of smart meter data has the potential to reveal personal information about what takes place in a person's home. Requiring law enforcement officials to obtain a warrant before accessing smart meter data is the best way to properly balance the government interest in investigating crimes while protecting a fundamental liberty recognized by the Fourth Amendment.

SARAH MURPHY*

[320] *See id.* (emphasizing the importance of the warrant requirement to Fourth Amendment jurisprudence).

* CIPP/US, J.D. Candidate, Boston College Law School (2020), B.S., Industrial Engineering, Clemson University (2017). I would like to thank Professor Robert Bloom for his indispensable guidance, feedback, and encouragement. I would also like to thank Professor Sayoko Blodgett-Ford for her editorial feedback and for helping to cultivate my interest in these important privacy issues.