THE IMPACT OF *CARPENTER V. UNITED STATES* ON DIGITAL AGE TECHNOLOGIES

APARNA BHATTACHARYA

I. INTRODUCTION

The past fifty years have been shaped by major advancements in technology that enable us to transfer information more freely and quickly than ever before. This digital age, however, has made it remarkably easier for third parties to collect a wealth of data on individuals based on the information we willingly share. These advancements have had substantial implications on privacy law, as the judiciary struggles to interpret antiquated laws with regard to previously inconceivable technologies. In June 2018, the Supreme Court handed down a landmark decision in *Carpenter v. United States*,[1] which changed the way the Fourth Amendment is applied to new and disruptive technologies. In making this decision, the Court recognized that in the last decade, technological advancements have made personal information exponentially more accessible to law enforcement officials than in prior years. In order to uphold the Founding-era principles that govern the Fourth Amendment and to protect the right of the people against unreasonable searches and seizures,[2] the test for what constitutes a search must be re-examined and must adapt to new societal expectations of what is considered reasonable.

Previously, the test for what constitutes a search focused on the places and items in which people have a reasonable expectation of privacy.[3] Under *Carpenter*, there is an increased focus on the technology itself—how advanced it is, what information it can reveal about our lives, and how it collects and stores that information.[4] If the technology enables a "too permeating police surveillance,"[5] it likely warrants *Carpenter*-protection and will be deemed an unreasonable search. In this Note, I discuss the three-pronged framework that can be deduced from *Carpenter*, and I apply it to other technologies developed in the digital age that generate records that have the potential to be just as revealing as the historical cell-site location information ("CSLI") at issue in *Carpenter*. These technologies include smart meters, pole cameras, and internet protocol ("IP") addresses. I ultimately argue that, while smart meters meet the three requirements of the framework, pole cameras and IP addresses are not "seismic shifts in digital

[1] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[2] *See* U.S. CONST. amend. IV.
[3] Orin S. Kerr, *Implementing Carpenter*, THE DIGITAL FOURTH AMENDMENT (forthcoming) (manuscript at 1), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257 (summarizing the well-accepted test derived from Justice Harlan's concurrence in Katz v. United States, 389 U.S. 347, 361 (1967)).
[4] *See generally Carpenter*, 138 S. Ct. 2206.
[5] *Id*. at 2214.

technology"[6] that create "an entirely different species"[7] of data essential for additional Fourth Amendment protections.

II. CARPENTER V. UNITED STATES

A. CASE BACKGROUND

First, it is important to understand the circumstances in *Carpenter* that led the Supreme Court to usher in such a novel change to its Fourth Amendment jurisprudence. In 2011, four men were arrested in connection with a string of robberies at Radio Shack and T-Mobile stores in Detroit.[8] One member of the group, Timothy Carpenter, confessed to the robberies and further admitted to robbing nine other stores in Michigan and Ohio over the previous four months.[9] He identified several accomplices who participated in the robberies and provided the FBI with his own cell phone number as well as some of the cell phone numbers of the identified accomplices.[10] The FBI also reviewed Carpenter's "call records to identify additional numbers that he had called around the time of the robberies."[11]

Prosecutors used this information to apply for court orders to obtain cell phone records for several suspects, including Carpenter, under 18 U.S.C. §2703(d) (2019), the Stored Communications Act.[12] The Stored Communications Act enables a governmental entity to "require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)"[13] if the governmental entity "offers specific and articulable facts showing that there are reasonable grounds to believe" that such records "are relevant and material to ongoing criminal investigation."[14] In other words, the government can obtain an individual's records without a warrant or probable cause if they can show that the evidence is reasonably related to a criminal investigation.

A federal magistrate judge found that the requirements of § 2703(d) had been met and ordered Carpenter's wireless carriers, Metro PCS and Sprint, to provide Carpenter's cell phone records for the four-month period during which the robberies took place.[15] The orders requested "152 days of cell-site records from MetroPCS, which produced records spanning 127 days[,]" as well as "seven days of CSLI from Sprint, which produced two days of records covering the period when Carpenter's phone was 'roaming' in northeastern Ohio."[16] As a result of the orders, the Government was able to

[6] *Id*. at 2219.
[7] *Id*. at 2222.
[8] *Id*. at 2212.
[9] *Id*.
[10] *Id*.
[11] *Id*.
[12] *Id*.
[13] 18 U.S.C. § 2703(c) (2019).
[14] 18 U.S.C. § 2703(d) (2019).
[15] *Carpenter*, 138 S. Ct. at 2212.
[16] *Id*.

obtain "12,898 location points cataloging Carpenter's movements—an average of 101 data points per day."[17]

Carpenter was eventually "charged with six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence" under 18 U.S.C. §§ 924(c) and 1951(a).[18] Before trial, "Carpenter moved to suppress the cell-site data provided by the wireless carriers" on the grounds that "the Government's seizure of the records violated the Fourth Amendment because they had been obtained without a warrant supported by probable cause. The District Court denied the motion."[19] At trial, an FBI agent's expert testimony was offered to show "that each time a cell phone taps into the wireless network, the carrier logs a time-stamped record of the cell site and particular sector that were used. With this information, [the agent] produced maps that placed Carpenter's phone near four of the charged robberies."[20] The Government relied on this information to prove Carpenter's proximity to the crimes and, therefore, his culpability.[21] Carpenter was convicted and sentenced to over one hundred years in prison.[22]

The United States Court of Appeals for the Sixth Circuit affirmed the trial court's decision on the grounds "that Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had [voluntarily] shared that information with his wireless carriers."[23] Relying on the third-party doctrine underscored in *Smith v. Maryland*,[24] the Sixth Circuit determined that the CSLI business records are not protected by the Fourth Amendment.[25] The Court reasoned that Carpenter should have known "that the wireless carriers have 'facilities for recording' locational information and that the 'phone company does in fact record this information for a variety of legitimate business purposes.'"[26] The Supreme Court granted Carpenter's petition for certiorari in 2017.[27]

B. SUPREME COURT DECISION

In a 5-4 decision, the Supreme Court reversed the judgment of the Sixth Circuit.[28] In doing so, the Court acknowledged that the existing Fourth Amendment tests must adapt to the change in the technological landscape of the digital age.[29] Chief Justice Roberts, writing for the majority, began with

---

[17] *Id*.
[18] *Id*. *See generally* 18 U.S.C. §§ 924(c), 1951(a) (2019).
[19] *Carpenter*, 138 S. Ct. at 2212.
[20] *Id*. at 2212–13.
[21] *See id*. at 2213.
[22] *Id*.
[23] *Id*.
[24] 442 U.S. 735 (1979).
[25] United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016).
[26] *Id*. (quoting *Smith*, 442 U.S. at 742, 745). *Smith* is a particularly noteworthy application of the traditional third-party doctrine. In *Smith*, the Supreme Court determined that telephone users likely do not have an expectation of privacy in the phone numbers they dial because this information is voluntarily revealed to the phone company. Phone users "know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes." *Smith*, 442 U.S. at 743.
[27] *Carpenter*, 138 S. Ct. at 2213.
[28] *Id*. at 2223.
[29] *See id*.

a discussion of how the Fourth Amendment has evolved since its inception in colonial times.[30] He stressed that "no single rubric definitively resolves which expectations of privacy are entitled to protection," but that an understanding of the Fourth Amendment's underlying purpose has guided the judicial system's interpretation of what constitutes unreasonable searches and seizures:[31] "First, that the Amendment seeks to secure 'the privacies of life' against 'arbitrary power[,]'"[32] and "[s]econd . . . that a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'"[33]

Chief Justice Roberts uses these "Founding-era understandings" to justify the Court's application of the Fourth Amendment to other "innovations in surveillance tools[,]" such as a thermal imager (as in *Kyllo v. United States*[34]) and cell phone contents (as in *Riley v. California*[35]).[36] In *Kyllo*, for example, the Supreme Court held that using an external thermal-imaging device aimed at a private home to detect heat from halide lamps used to grow marijuana within the home constituted a search.[37] Any alternative approach "would leave homeowners at the mercy of advancing technology."[38] In arriving at its decision in *Carpenter*, the Court again found that advancements in technology merited another adjustment to the way searches are analyzed under the law.

Instead of simply focusing on whether an individual has a reasonable expectation of privacy in places or things, the Court looked to whether "technology changed expectations of *what the police can do*."[39] Before modern innovations in surveillance technology, pursuing a suspect "for an extended period of time was 'difficult and costly and therefore rarely undertaken.'"[40] With access to the CSLI, the FBI was able to retroactively track Carpenter's location over a prolonged period of time.[41]

The Court deemed this "near perfect surveillance."[42] They further characterized the historical cell phone records as "detailed, encyclopedic, and effortlessly compiled."[43] Access to this breadth of historical data and granular detail goes beyond information that is reasonably required to pursue a criminal investigation. It "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, and sexual associations.'"[44]

Furthermore, there was a departure from the traditional understanding of the third-party doctrine. The text of the Fourth Amendment states that people

---

[30] *Id*. at 2213.
[31] *Id*. at 2213–14.
[32] *Id*. at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).
[33] *Id*. (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).
[34] Kyllo v. United States, 533 U.S. 27 (2001).
[35] Riley v. California, 573 U.S. 373 (2014).
[36] *Carpenter*, 819 F.3d at 2114.
[37] *Kyllo*, 533 U.S. at 29–30.
[38] *Id*. at 35; *see also* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).
[39] Kerr, *supra* note 3 (manuscript at 7).
[40] *Carpenter*, 138 S. Ct. at 2217 (quoting United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring)).
[41] *See id*. at 2218.
[42] *Id*.
[43] *Id*. at 2216.
[44] *Id*. at 2217 (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

have a right to be "secure in *their* . . . papers."[45] The Supreme Court referred to its prior holdings in *Smith v. Maryland*[46] and *United States v. Miller*[47] and explained that this means that a person essentially does not have a "legitimate expectation of privacy in information he voluntarily turns over to third parties"[48] regardless of whether a person discloses such information under the "assumption that it will be used only for a limited purpose."[49] Thus, the government can obtain this information directly from third parties without having probable cause or obtaining a warrant. The Supreme Court, however, declined to extend *Smith* and *Miller* in this case because these decisions were made prior to the "seismic shifts in digital technology" that CSLI represents.[50] Wireless carriers "casually"[51] collect a "detailed chronicle of a person's physical presence . . . every day, every moment, over several years."[52] Moreover, the Court did not feel that individuals' locational information is shared truly *voluntarily* with wireless carriers because "cell phones . . . are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[53] They are able to log CSLI records "without any affirmative act on the part of the user beyond powering up."[54] While individuals voluntarily use their cell phones to store and communicate private information, the use itself should not sacrifice their expectation of privacy.

For these reasons, the Supreme Court decided that the government's acquisition of cell-site records without a warrant constituted a search under the Fourth Amendment.[55] The Court stressed that *Carpenter* is a narrow decision that does not disturb *Smith* and *Miller* nor does it "address other business records that might incidentally reveal location information."[56] However, the analysis in this case certainly has implications for other technologies that emerged in the digital era. In Part III, I discuss a possible post-*Carpenter* framework to apply to some of these technologies.

III. CARPENTER FRAMEWORK

Katz v. United States remains the prevailing precedent establishing an individual's reasonable expectation of privacy in relation to electronic surveillance.[57] In *Katz*, the Supreme Court considered whether a defendant's

---

[45] U.S. CONST. amend. IV (emphasis added).
[46] Smith v. Maryland, 442 U.S. 735 (1979).
[47] United States v. Miller, 425 U.S. 435 (1976).
[48] *Carpenter*, 138 S. Ct. at 2216 (quoting *Smith*, 442 U.S. at 743–44).
[49] *Id.* (quoting *Miller*, 425 U.S. at 443). In *Miller*, the Supreme Court rejected a Fourth Amendment challenge to a third-party subpoena for the defendant's bank records because the documents "contain[ed] information voluntarily conveyed to the banks and [were] exposed to [bank] employees in the ordinary course of business." *Miller*, 425 U.S. at 442.
[50] *Carpenter*, 138 S. Ct. at 2219.
[51] *Id.*
[52] *Id.* at 2220.
[53] *Id.*
[54] *Id.*
[55] *Id.* On remand, the Sixth Circuit determined that the CSLI was permitted to come into evidence under the good-faith doctrine because the FBI reasonably relied on the Stored Communications Act. United States v. Carpenter, 926 F.3d 313, 314 (6th Cir. 2019). As a result, Carpenter's conviction by the district court was ultimately affirmed. *Id.* at 318.
[56] *Carpenter*, 138 S. Ct. at 2220.
[57] Katz v. United States, 389 U.S. 347 (1967).

Fourth Amendment rights were implicated when FBI agents "attached an electronic listening and recording device to the outside of the public telephone booth from which [the defendant] had placed his calls."[58] The Court ultimately ruled that this constituted a search. In Justice Stewart's majority opinion, he states that "the Fourth Amendment protects *people*, not places."[59] However, Justice Harlan's concurrence, which ultimately became the predominant test, established a two-prong test that required both an individual's subjective expectation of privacy and an objective reasonable expectation of privacy in a particular *place*.[60] He emphasized that "reference to a 'place'" is required in determining the protections afforded to people under the Fourth Amendment.[61] Since *Katz* was decided in 1967, case law on the Fourth Amendment centered on whether individuals have a right to privacy in both places and things.[62]

The decision in *Carpenter* altered the approach to understanding an individual's expectation of privacy; it "focuses on how much the government can learn about a person regardless of the place or thing from which the information came."[63] Professor Orin Kerr[64] neatly defines three requirements necessary for a category of records to be able to gain Fourth Amendment protection under *Carpenter*: (1) "the collection of information [must have been] made widely possible by surveillance methods of the digital age"; (2) "the records must not be the product of a user's meaningful voluntary choice"; and (3) "the records must be of a type that tends to reveal an intimate portrait of a person's life beyond the legitimate interests of criminal investigations . . . , such as our personal associations, religious beliefs, sexual preferences, and political views."[65]

The first requirement—that the records have been made available because of digital technology—leads to somewhat of a judgment call. In *Carpenter*, Chief Justice Roberts stressed that the majority's opinion narrowly applies to "seismic shifts in digital technology"[66] rather than "call[ing] into question conventional surveillance techniques and tools, such as security cameras."[67] They point out that "[t]here is a world of difference between the limited types of personal information" that could previously be collected and the "exhaustive chronicle" of information "casually collected" today.[68] The Court's characterizations of CSLI as "an entirely different species of business record"[69] indicates that in order to receive *Carpenter*-protection, the technology at issue must be novel or highly transformative; early surveillance tools, despite their potentially revealing nature, cannot

[58] *Id*. at 348.
[59] *Id*. at 351 (emphasis added).
[60] *Id*. at 361.
[61] *Id*. (Harlan, J., concurring); *see also* Peter Winn, *Katz and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 7 (2008).
[62] *See* Kerr, *supra* note 3 (manuscript at 6).
[63] *Id*.
[64] Orin Kerr is a Professor at the University of California, Berkeley School of Law, who specializes in criminal procedure and computer crime law. He previously served as the Francis R. and John J. Duggan Distinguished Professor at the University of Southern California Gould School of Law.
[65] Kerr, *supra* note 3 (manuscript at 3).
[66] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).
[67] *Id*. at 2220.
[68] *Id*. at 2219.
[69] *Id*. at 2221.

qualify.[70] However, it can be difficult to determine which technologies should be included or excluded when significant advancements have been made to existing, older technologies over time.

The second requirement—that the records must not be the product of the user's meaningful voluntary choice—challenges the traditional application of the third-party doctrine in the context of digital technologies.[71] The Court asserts that carrying a cell phone is "indispensable to participation in modern society."[72] Because of this, "that gives you no real choice whether to disclose your location."[73] In evaluating which technologies may qualify as indispensable to participation in modern society, Kerr urges us to make three judgment calls: "First what does modern society look like; second, what does it mean to participate in that society; and third what technologies are needed to achieve that participation."[74] Additionally, he suggests that *Carpenter* has a "compulsion requirement."[75] In other words, individuals must volunteer to reveal information that goes "beyond what the technology requires" in order to be a "meaningful voluntary" disclosure.[76] Thus, the simple use of a phone triggering the collection of CSLI is not the same as a user making an affirmative decision to share that CSLI with a wireless carrier.

Finally, the third requirement—that the collected records reveal intimate information beyond the interests of criminal investigations—harkens back to one of the goals of the Fourth Amendment in "secur[ing] 'the privacies of life' against 'arbitrary power.'"[77] Such intimate information can include "not only [an individual's] particular movements" but also their "familial, political, professional, religious, and sexual associations."[78]

In applying this framework, I focus on the "Source Rule." Under this rule, "government access to *any* information that owes its source to *Carpenter*-protected information is a search."[79] For example, "access to any time period of a person's cell-site records would be a search" as would

---

[70] *See* Kerr, *supra* note 3 (manuscript at 17). "For example, it's surely invasive for the police to obtain all of your bank records so they can examine your financial transactions and learn what you bought and from whom." *Id.*; *see also* United States v. Miller, 425 U.S. 435 (1976). Kerr explains that this distinction makes sense because *Carpenter* is premised on "the theory that digital records are categorically different" from "their pre-digital equivalents." Kerr, *supra* note 3 (manuscript at 17). *Carpenter* signals that seismic shifts in technology justify a departure from the treatment of earlier, conventional surveillance technologies. Therefore, it would be illogical to conclude that earlier tools warrant *Carpenter*-protection if they existed in the pre-digital age. Additionally, this distinction is "consisten[t] with the theory of equilibrium-adjustment." *Id.* (manuscript at 18). The equilibrium-adjustment theory suggests that the judiciary responds to "changing technology and social practice[s]. When new tools and new practices threaten to expand or contract police power in a significant way, courts adjust the level of Fourth Amendment protection to try to restore the prior equilibrium." Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011). Because earlier technologies could only collect and store a limited amount of data, that was all that was available to the investigating authorities. Thus, individuals' expectations of what the government could learn about them was limited. However, the increased availability of personal information should not mean that individuals should adjust their expectations of privacy in this information.

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

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

[73] Kerr, *supra* note 3 (manuscript at 21).

[74] *Id.*

[75] *Id.* (manuscript at 21–22).

[76] *Id.*

[77] *Carpenter*, 138 S. Ct. at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

[78] *Id.* at 2217 (quoting in United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

[79] Kerr, *supra* note 3 (manuscript at 41) (emphasis added).

"[l]earning if the phone was in the state of California on a particular date."[80] Alternative approaches, including the "Subjective Approach" and the "Mosaic Theory," are not considered in this note.[81]

IV. APPLICATION TO SMART METERS

One form of technology to consider is the smart meter. Such innovative devices are becoming increasingly prevalent as cities, states, and countries roll out "Smart Grid" initiatives to allow both suppliers and users to monitor and control energy consumption. However, the technology used to survey the records of individuals' energy consumption patterns also presents a number of challenges including newly emerging privacy concerns. Smart meters have already been considered by the judiciary since *Carpenter* was decided in *Naperville Smart Meter Awareness v. City of Naperville*.[82] In this case, the Seventh Circuit cited several studies on smart meter data collection to support its opinion that the collection of energy consumption data by smart meters constitutes a search.[83] However, the opinion reflects a very cursory analysis of each of these studies. Thus, it is important to understand the technology more thoroughly in order to see if smart meters truly should qualify for additional Fourth Amendment protections.

A. TECHNOLOGY OVERVIEW

An energy meter is a device that measures the amount of electric energy consumed by a building, tenant space, or electrically powered equipment.[84] They are installed at customers' premises to allow energy suppliers to measure consumption for billing purposes.[85] The early, traditional analog meters stored consumption data locally. Utility employees typically had to visit homes, generally on a monthly basis, to manually read the devices to retrieve a "single lump-sum" of energy consumption records.[86] Eventually energy suppliers were able to use automatic meter reading devices ("AMR"), which "periodically report electricity use to utilities from mechanical meters with an electronic signal."[87] However, these readers are limited in that they only communicate the data to suppliers on a daily, weekly, or monthly basis.[88]

By contrast, a smart meter, or an advanced meter, is "a metering system that records customer consumption (and possibly other parameters) hourly

---

[80] *Id*.

[81] *See* Kerr, *supra* note 3 (manuscript at 27). The Subjective Approach "focus[es] on when the government learned the kind of private information that *Carpenter* safeguards" while the Mosaic Theory "focus[es] instead on whether the quantity of records obtained are ordinarily sufficient to reveal the kinds of private information that animated *Carpenter*." *Id*.

[82] Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521 (7th Cir. 2018).

[83] *See Naperville*, 900 F.3d at 525–27.

[84] *What is an Electric Meter?*, ENERTIV (Jan. 16, 2019), https://www.enertiv.com/resources/faq/what-is-electric-meter.

[85] *Id*.

[86] *Electricity Explained: Measuring Electricity*, U.S. ENERGY INFO. ADMIN. (Jan. 8, 2020), https://www.eia.gov/energyexplained/index.php?page=electricity_measuring.

[87] *Id*.

[88] *What is the Difference Between AMR Devices and Smart Meters?*, GAZPROM ENERGY (Sept. 21, 2015), https://www.gazprom-energy.co.uk/blog/what-is-the-difference-between-an-amr-and-a-smart-meter/.

or more frequently and provides for daily or more frequent transmittal of measurements over a communication network to a central collection point."[89] The communication network consists of a wide area network ("WAN"), a neighborhood area network ("NAN"), and a home area network ("HAN").[90] Communication is made possible at the HAN level through these individual networks' use of smart devices deployed at customer premises;[91] at the NAN level through wireless or wired technologies including power lines, DSL, Broadband, Wi-Fi, and copper and fiber cables;[92] and at the WAN level through power line communication, fiber optics, and wireless technologies.[93] Unlike AMR, this communication is bi-directional.[94]

Simply put, smart meters measure energy use and frequently communicate that information directly to *both* the user and energy supplier via internet and powerline communication networks. This enables precise monitoring for consumers to adjust behavior and for utility companies to regulate prices.

Smart meters are part of a larger advanced metering infrastructure ("AMI"), which is a collection of technologies aimed at furthering Smart Grid goals including reliability, adaptability, and prediction in energy consumption.[95] AMI represents monumental innovation in the energy industry. AMI, and particularly smart meters, provide a number of functions that were not previously possible through traditional metering infrastructures.

Smart meters enable users and suppliers to automatically and remotely "measure electricity consumption in real-time[,]"[96] as well as "connect and disconnect service, detect tampering, identify and isolate outages, and monitor voltage."[97] They can record consumption much more frequently than traditional meters, "often collecting thousands of readings every month."[98] In fact, "some smart meters can even measure the electricity use of *individual* devices[,]"[99] whereas conventional meters could only measure and display *aggregate* consumption levels.[100] From this data, utility companies are able to determine "both the amount of electricity being used inside a home and when that energy is used."[101]

In *Naperville*, the Seventh Circuit relied on a study by Ramyar Rashed Mohassel et al. titled *A Survey on Advanced Metering Infrastructure*.[102] In

---

[89] FED. ENERGY REG. COMM'N, ASSESSMENT OF DEMAND RESPONSE & ADVANCED METERING STAFF REPORT 5 (Dec. 2008), https://www.ferc.gov/legal/staff-reports/12-08-demand-response.pdf.

[90] *See generally* MOHAMMED F. KHAN ET AL., COMM. TECHS' FOR SMART METERING INFRASTRUCTURE (2014).

[91] *Id*. at 4.

[92] *Id*. at 3.

[93] *Id*.

[94] Ramyar Rashed Mohassel et al., *A Survey on Advanced Metering Infrastructure*, 63 INT'L J. ELECTRICAL POWER & ENERGY SYS. 473, 475 (2014).

[95] *Id*. at 474.

[96] *Electricity Explained: Measuring Electricity*, *supra* note 86.

[97] U.S. DEP'T OF ENERGY, ADVANCED METERING INFRASTRUCTURE AND CUSTOMER SYSTEMS: RESULTS FROM THE SMART GRID INVESMENT GRANT PROGRAM 4 (Sept. 2016), https://www.energy.gov/sites/prod/files/2016/12/f34/AMI%20Summary%20Report_09-26-16.pdf.

[98] Naperville Smart Meter Awareness v. Naperville, 900 F.3d 521, 524 (7th Cir. 2018).

[99] *Electricity Explained: Measuring Electricity*, *supra* note 86 (emphasis added).

[100] Mohassel et al., *supra* note 94, at 478.

[101] *Naperville*, 900 F.3d at 524.

[102] *Id*.

this study, Mohassel discusses the role of AMI in smart grid initiatives, including the numerous security challenges that AMI presents.[103] According to Mohassel, individual appliances have "load signatures" with distinct characteristics like voltage, current, and energy or power.[104] These signatures make it "possible to perform 'consumer profiling' with an alarmingly high accuracy. Examples range from how many people live in the house, duration of occupancy, type of appliances, security and alarming systems, to inferring special conditions such as medical emergencies . . . ."[105] In fact, it is also possible to glean this information from the smart meter records alone, "even without utilization of sophisticated algorithms and computer aided tools."[106] However, Mohassel also notes that there is a technique known as "load signature moderation," which "basically re-shapes the overall pattern of data to make distinguishing load patterns and signatures impossible."[107]

The Naperville court also heavily relied upon another study, titled *A Neuron Nets Based Procedure for Identifying Domestic Appliances Pattern-of-Use from Energy Recordings at Meter Panel*, by A. Prudenzi.[108] Prudenzi confirms Mohassel's discussion about distinct appliance load signatures.[109] In this article, Prudenzi indicates that analyzing energy recordings at intervals of ten to fifteen minutes can provide information that identifies appliance patterns-of-use.[110] He breaks down the typical energy consumption patterns of the most commonly used appliances including refrigerators, freezers, washing machines, and dishwashers.[111] It is clear that each appliance consumes a distinctly different amount of energy.[112] As a result, researchers can use this data to "predict the appliances that are present in a home and when those appliances are used."[113] "The accuracy of these predictions depends, of course, on the frequency at which the data is collected and the sophistication of the tools used to analyze that data."[114]

B. *CARPENTER* APPLICATION

Utility records traditionally received Fourth Amendment treatment similar to bank records and telephone records in that courts have found that customers do not have a reasonable expectation of privacy in such records.[115] For example, in *United States v. Starkweather*, the Ninth Circuit found that there was "no principled reason to accord electric utility records any different status under the Fourth Amendment than that accorded bank or telephone records" and that public awareness that such records are maintained negates

[103] *See generally* Mohassel et al., *supra* note 94.
[104] *Id*. at 478.
[105] *Id*.
[106] *Id*.
[107] *Id*.
[108] Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 524–26 (7th Cir. 2018).
[109] *See generally* A. Prudenzi, *A Neuron Nets Based Procedure for Identifying Domestic Appliances Pattern-of-Use from Energy Recordings at Meter Panel*, 2 IEEE POWER ENGINEERING SOC'Y WINTER MEETING 941 (2002).
[110] *Id*. at 941.
[111] *Id*. at 942.
[112] *See id*.
[113] *Id*.
[114] Naperville Smart Meter Awareness v. Naperville, 900 F.3d 521, 524 (7th Cir. 2018).
[115] CONG. RES. SERV. (CRS), SMART METER DATA: PRIVACY AND CYBERSECURITY 15 (2012).

any expectation of privacy.[116] The Eighth Circuit came to a similar conclusion about such records in *United States v. McIntyre*, distinguishing *Kyllo* by arguing that the thermal imaging devices in *Kyllo* were far more intrusive than the electricity usage records in *McIntyre*.[117]

However, these decisions were made prior to the staggering technological advancements and prevalence of smart meters in the industry. In 2007, there were only about seven million smart meter installations in the United States.[118] In 2016, there were about seventy-one million installed, encompassing 47 percent of the 150 million electricity customers in the U.S.[119] In 2020, it is expected that there will be ninety million smart meters installed.[120] As a result of this innovation, the technology needs to be re-examined under the Fourth Amendment to determine whether smart meters should receive an additional layer of protection. Applying the three requirements under the *Carpenter* framework, the collection of digital smart meter records should trigger a search that requires a warrant.

First, I consider whether the collection of such detailed energy consumption records was made possible by the digital age. Given the transformative nature of smart meters as compared to traditional analog meters, it seems likely that this prong of the test is met. With traditional analog meters, generally only *monthly* electricity usage data could be examined as a single lump-sum figure by an in-person meter reader.[121] These readings were incapable of distinguishing between which appliances were functioning or present at any given point.[122] Technology now allows utility providers real-time monitoring capabilities over individuals' utility usage using internet and powerline communication networks.[123] Furthermore, an analysis of smart meter records of load signatures can reveal exactly which appliances are present in households and when they are being used.[124] The result is that utility networks are able to collect vastly more (and much more precise) data points of electricity usage than with earlier meter versions. Therefore, smart meters should be classified as a digital age technology that satisfies the first prong of the *Carpenter* framework.

Second, energy-consumption records are created without any meaningful voluntary choice of the user. In many cases, replacing analog meters with smart meters is not a choice.[125] In *Naperville*, for example, Naperville residents were not given the option to opt out of a smart meter

---

[116] United States v. Starkweather, No. 91-30354, 1992 WL 204005, at *2 (9th Cir. Aug. 24, 1992); *see also* CONG. RES. SERV. (CRS), *supra* note 115, at 15.

[117] United States v. McIntyre, 646 F.3d 1107, 1111 (8th Cir. 2011); *see also* CONG. RES. SERV. (CRS), *supra* note 115, at 15.

[118] ADAM COOPER, ELECTRIC COMPANY SMART METER DEPLOYMENTS: FOUNDATION FOR A SMART GRID 2 (Oct. 2016).

[119] *Nearly Half of All U.S. Electricity Customers Have Smart Meters*, U.S. ENERGY INFO. ADMIN. (Dec. 6, 2017), https://www.eia.gov/todayinenergy/detail.php?id=34012.

[120] *Number of Electric Smart Meters Installations Deployed in the U.S. from 2007 to 2020 (in million units)*, STATISTA, https://www.statista.com/statistics/676472/number-of-smart-meter-installations-in-the-united-states/ (last visited Apr. 1, 2020).

[121] *See supra* Part IV.A.

[122] *See supra* Part IV.A.

[123] *See supra* Part IV.A.

[124] *Supra* Part IV.A.

[125] *See, e.g.*, Naperville Smart Meter Awareness v. Naperville, 900 F.3d 521, 524 (7th Cir. 2018); Wade v. Ill. Commerce Comm'n, 91 N.E.3d 383, 385 (Ill. App. Ct. 2017).

program after the city began replacing residents' analog meters with smart meters as part of an effort to update the city's electrical grid.[126] Additionally, it is possible that residential customers are not even *aware* that they have a smart meter installed. A Residential Energy Consumption Survey reported that "in 2015, a year when residential smart meter adoption was about 44% nationwide . . . 22% of households reported having a smart meter, 49% reported not having one, and 29% responded that they did not know."[127]

Furthermore, using electricity is equally as "indispensable to participation in modern life,"[128] if not more so, than using a cell phone. The use of appliances—washing machines, refrigerators, microwaves, ovens, dishwashers—is a part of everyday life. "[A] home occupant does not assume the risk of near constant monitoring by choosing to have electricity in her home."[129] The decision to use a washing machine should not insinuate a voluntary disclosure to utility providers through the traditional third-party doctrine analysis proffered by *Smith* and *Miller*. Although consumers recognize that utility providers collect energy consumption data for legitimate business purposes, such as billing, that does not mean that consumers have consented to the collection of such detailed and revealing records for the purposes of a governmental search.

Third, records from smart meters tend to reveal an intimate portrait of a person's life. Previous case law has stressed that "*all* details are intimate details" in the context of protecting the sanctity of a home from a search.[130] Here, however, the analysis focuses on the level of detail that smart meters can reveal about individuals. In other words, the fact that this information is collected in an individual's home is secondary to smart meters' revealing nature. Detailed consumer profiles can be drawn from appliances' load signatures.[131] With real-time data on electricity usage, utility companies and law enforcement officials may have the ability to monitor household activities and discern occupants' daily schedules.[132]

The Seventh Circuit addressed this issue in *Naperville*.[133] Relying on *Kyllo* and *Carpenter*, the court determined that the collection of residents' energy-usage data at fifteen-minute intervals, stored by the city for up to three years, constituted a search under the Fourth Amendment.[134] The court found that these smart devices give utility companies access to "intimate personal details of the City's electric customers such as when people are home and when the home is vacant, sleeping routines, eating routines, specific appliance types in the home and when used, and charging data for plug-in vehicles that can be used to identify travel routines and history."[135]

---

[126] *Naperville*, 900 F.3d at 524. Residents were able to request "non-wireless" smart meters, which did not transmit the data directly to the utility company; instead, the data had to be manually retrieved. However, these meters collected "equally rich data." *Id*. at n.1.

[127] *Nearly Half of All U.S. Electricity Customers Have Smart Meters*, *supra* note 119.

[128] Carpenter v. United States, 138 S.Ct. 2206, 2220 (2018).

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

[130] Kyllo v. United States, 533 U.S. 27, 37 (2001).

[131] *Supra* Part IV.A.

[132] CONG. RES. SERV. (CRS), *supra* note 115, at 5.

[133] *See Naperville*, 900 F.3d at 524.

[134] *Id*.

[135] *Id*. However, the Court ultimately found that this search was reasonable given the government's "substantial" interest in collecting this data, because of the significant benefits that smart meters offer, including allow[ing] utilities to reduce costs, provid[ing] cheaper power to consumers, encourag[ing]

This technology is at least as revealing as that found to be a search in *Kyllo*, which merely revealed that a home was emanating a certain amount of heat.[136]

There are strong justifications for an expectation of privacy in activities stemming from electricity usage. Smart meters enable third parties to collect deeply personal information about users. How much television does a person watch? How often do they wash their clothes? When are they home alone, and when are guests present? Why do they need so many medical devices? These records clearly divulge information well beyond the legitimate interests of government investigations. Therefore, anything stemming from the collection of smart meter records should receive *Carpenter*-protection under the Fourth Amendment, leaving energy consumption data free from a warrantless search.

Naperville suggests that this analysis could change once the use of smart meters becomes even more widespread. Relying on *Kyllo*, the Seventh Circuit stated that "even an extremely invasive technology can evade the warrant requirement if it is 'in general public use.'"[137] But the use of smart meters is "not yet so pervasive that they fall into this class."[138] Therefore, even if a technology is deeply revealing, there may not be limitations on the government's collection of its records if the technology is commonly used. The court does not clarify when this threshold will be met. Given the pervasiveness of cell phone use in society and the decision in *Carpenter*, however, this is likely to be a long way off for smart meters.

V. POLE CAMERAS

Another technology to consider is a pole, or IP, camera. Traditionally, video surveillance does not trigger a constitutional concern when an individual is recorded in a public space,[139] such as a public park, sidewalk, street, or area outside the curtilage of a house not commonly accessible to the public.[140] The Supreme Court has also held in *California v. Ciraolo*[141] that the Fourth Amendment is not violated by a warrantless aerial observation of a fenced-in backyard within the curtilage of a home[142] because the area in question was "readily discernible to the naked eye[,]"[143] and the Fourth Amendment "has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."[144] An

energy efficiency, and increas[ing] grid stability." *Id*. at 529. The Court emphasized that this holding is limited to situations in which "the search is unrelated to law enforcement, is minimally invasive, and presents little risk of corollary criminal consequences." *Id*.

[136] *See id*. at 526; *see also* Orin Kerr, *Public Utility's Recording of Home Energy Consumption Every 15 Minutes is a 'Search,' Seventh Circuit Rules*, LAWFARE (Aug. 17, 2018, 12:29 PM), https://www.lawfareblog.com/public-utilitys-recording-home-energy-consumption-every-15-minutes-search-seventh-circuit-rules.

[137] *Naperville*, 900 F.3d at 526 (quoting Kyllo v. United States, 533 U.S. 27, 40 (2001)).

[138] *Id*. at 527.

[139] Tiffany M. Russo, *Searches and Seizures as Applied to Changing Digital Technologies: A Look at Pole Camera Surveillance*, 12 SETON HALL CIR. REV. 114, 115 (2015).

[140] IRS, PRIVACY IMPACT REPORT OF IP CAMERA SYSTEMS (2016), https://www.irs.gov/pub/irs-utl/ip-camera-systems-pia.pdf.

[141] California v. Ciraolo, 476 U.S. 207 (1986).

[142] *Id*. at 215.

[143] *Id*. at 213.

[144] *Id*.

issue can arise in situations in which a reasonable expectation of privacy concern is "attached to the area being monitored."[145]

However, the analysis under *Carpenter* asks how much information we can learn about an individual from the *technology itself* rather than questioning the thing or place from which the information came.[146] Given the vast level of information that pole camera systems can collect and store, this technology is worth reviewing under the *Carpenter* framework to determine whether it should qualify for additional Fourth Amendment protections.

A. TECHNOLOGY OVERVIEW

Video surveillance has been used since the early twentieth century.[147] The world's first network camera was invented in 1996; it "transform[ed] video surveillance from analog to digital."[148] These "first generation" IP cameras "were designed to be mounted on utility poles and street lights."[149] Newer versions of IP cameras "come in many configurations . . . . However, the term 'pole cam' is still in use to refer to IP cameras in general."[150]

Pole cameras are covert video surveillance systems used by law enforcement to conduct extended surveillance in criminal investigations.[151] Generally, law enforcement will use pole cameras "when it is operationally impractical to conduct physical surveillance or where suspects engage in counter-surveillance."[152] They are "used for situations that require long-term surveillance and would result in a significant amount of human resource hours or in situations in which it is not safe to conduct a human surveillance."[153] Pole camera systems "can be easily and quickly mounted on a pole or structure that has access to power."[154] Typically, a utility pole owner will provide law enforcement officials with permission to affix the camera to a utility pole.[155] They tend to "offer wireless and cellular network communication options."[156] These cameras provide twenty-four-hour surveillance, have the ability to zoom in on areas of interest, and have day and night capabilities.[157]

Additionally, the image resolution of pole cameras has significantly increased in quality, as compared to analog video cameras. Analog video cameras continue to use a National Television Systems Committee ("NTSC") coloring system that is almost forty years old and "has well-

---

[145] Russo, *supra* note 139, at 115.

[146] *See supra* Part III.

[147] Rick Delgado, *From Edison to Internet: A History of Video Surveillance*, BUS. 2 COMMUNITY (Aug. 14, 2013), https://www.business2community.com/tech-gadgets/from-edison-to-internet-a-history-of-video-surveillance-0578308.

[148] *History*, AXIS COMMUNICATIONS, https://www.axis.com/about-axis/history (last visited Mar. 3, 2019).

[149] IRS, *supra* note 140.

[150] *Id*.

[151] *Id*.

[152] Russo, *supra* note 139, at 116.

[153] IRS, *supra* note 140.

[154] *How Deployable Pole Camera Systems Assist Law Enforcement*, I2C TECHS., https://www.i2ctech.com/pole-camera-systems-assist-law-enforcement/ (last visited Mar. 3, 2019).

[155] *See* Richard Lorenz, *Are Utility Pole-Mounted Cameras Unlawful?*, W. ENERGY INST. (June 13, 2016), https://www.westernenergy.org/news-resources/are-utility-pole-mounted-cameras-unlawful/.

[156] *How Deployable Pole Camera Systems Assist Law Enforcement*, *supra* note 154.

[157] *Covert Pole Cameras*, SUPER CIRCUITS, https://www.supercircuits.com/law-enforcement/field-surveillance-systems/covert-pole-cameras (last visited Mar. 3, 2019).

known performance limitations . . . [including] flickering and ghosting."[158] In contrast, "IP cameras come in a broad range of resolutions (measured in megapixels, or MP)."[159] Even the lowest resolution IP camera "has almost 4 times the resolution of an analog camera. With this added resolution, faces become clearer, license plates become easier to read and larger areas can be covered by a single camera."[160]

The most significant feature of modern pole cameras is the ability to access and view the recordings remotely.[161] Earlier video surveillance techniques required "an agent . . . to be in close proximity to a recording device to be able to view the video stream live or to retrieve the stored video . . . [, whereas] IP cameras transmit through cellular networks to the internet to stream live video surveillance."[162] The cameras can transmit the video footage to remote servers and investigators can access both a live video feed or previously-recorded footage from a mobile phone.[163] On the receiving end, the videos may be saved to "any standard storage media."[164]

Additional innovations to this technology include installing license plate recognition ("LPR") cameras to fixed pole video surveillance systems.[165] This gives law enforcement the ability to identify stolen vehicles. There are also cameras on the market that use facial recognition software.[166] Some countries have started to incorporate this software into pole cameras.[167] In Singapore, for example, the government plans to install these cameras in order "to 'perform crowd analytics' and support anti-terror operations."[168] Yitu Technology, a Chinese computer security service operating in Singapore, reports that "its facial recognition platform is capable of identifying over 1.8 billion faces in less than 3 seconds."[169] These advancements provide an indication of what technology is already on the market and how it may continue to grow in the future. However, the United States may not be as inclined to adopt such similar innovations. San Francisco, California, for example, was the first American city to ban the use of facial recognition software for government searches to mitigate individuals' privacy concerns.[170]

---

[158] Joseph Farrell & Carl Shapiro, *Standard Setting in High-Definition Television*, 23 BROOKINGS PAPERS: MICROECONOMICS 1, 1 (1992), https://www.brookings.edu/wp-content/uploads/1992/01/1992_bpeamicro_farrell.pdf.

[159] *Camera Solutions*, HARRIS SECURITY SYSTEMS: CAMERA SYSTEMS, www.harrissecurity.com/Commercial/Camera-Systems.

[160] *Id*.

[161] IRS, *supra* note 140.

[162] *Id*.

[163] State v. Jones, 903 N.W.2d 101, 104 (S.D. 2017).

[164] IRS, *supra* note 140.

[165] *License Plate Recognition Cameras*, MD. SECURITY PROFS., https://marylandsecurity.net/surveillance-systems/license-plate-recognition-cameras/ (last visited Mar. 3, 2019).

[166] *E.g.*, *FacePRO: Panasonic Facial Recognition System*, PANASONIC, https://security.panasonic.com/Face_Recognition/ (last visited Mar. 3, 2019).

[167] *See, e.g.*, Aradhana Aravindan & John Geddie, *Singapore to Test Facial Recognition on Lampposts, Stoking Privacy Fears*, REUTERS (Apr. 13, 2018), https://www.reuters.com/article/us-singapore-surveillance/singapore-to-test-facial-recognition-on-lampposts-stoking-privacy-fears-idUSKBN1HK0RV.

[168] *Id*.

[169] *Id*.

[170] Kate Conger et al., *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

B. *CARPENTER* APPLICATION

The Sixth Circuit considered pole camera surveillance in 2016—before *Carpenter* was handed down—in *United States v. Houston*.[171] A divided court determined that pole camera surveillance was not a search under the Fourth Amendment.[172] In *Houston*, law enforcement officials directed a utility company to "install[] a surveillance camera on a public utility pole . . . . The camera broadcasted its recordings via an encrypted signal to an IP address accessed through a log-in and password. The camera could move left and right and had a zoom function."[173] However, even with the advancements in this technology, the Sixth Circuit determined that the "agents only observed what [the defendant] made public to any person traveling on the [surrounding] roads . . . ."[174] Additionally, the court held that using video camera surveillance as opposed to stationing agents to conduct twenty-four hour surveillance on the suspect did not make the surveillance unconstitutional.[175] Judge Rogers, writing for the majority, explained that "the Fourth Amendment does not punish law enforcement for using technology to more efficiently conduct their investigations."[176] Post-*Carpenter*, there has been hesitation to extend the logic of *Carpenter* to pole cameras for similar reasons.

Whether pole cameras merit *Carpenter*–protection largely turns on the first prong of the framework: were pole camera surveillance records made possible as a result of the digital age? Courts seem wary of classifying it as such. In *United States v. Kay*, investigators used evidence from a pole camera to obtain a warrant to search a defendant's residence, where agents recovered distribution quantities of Oxycodone.[177] The defendant attempted to argue that *Carpenter* protects "advanced technology" against excessive police surveillance.[178] The court rejected this argument emphasizing that *Carpenter* was a limited decision and did "not . . . call into question conventional surveillance techniques and tools, such as security cameras."[179]

Similarly, in the Illinois district court case *United States v. Tuggle*, investigators maintained three pole cameras in the area surrounding the property of a defendant suspected of participating in a drug trafficking ring.[180] These cameras had "rudimentary lighting technology to assist the cameras' operation at night . . . [, and] [t]he surveillance footage was viewable in real time" from a remote location.[181] However, "[t]he cameras could not record audio, nor did they have infrared or any capabilities to view or capture anything inside the Defendant's residence that he did not expose

---

[171] United States v. Houston, 813 F.3d 282 (6th Cir. 2016).
[172] *Id*. at 287–88.
[173] *Id*. at 286.
[174] *Id*. at 288.
[175] *Id*.
[176] *Id*.
[177] United States v. Kay, No. 17-CR-16, 2018 WL 3995902, at *1 (E.D. Wis. Aug. 21, 2018); *see also* Nathaniel Sobel, *Four Months Later, How Are Courts Interpreting Carpenter?*, LAWFARE (Oct. 18, 2018), https://www.lawfareblog.com/four-months-later-how-are-courts-interpreting-carpenter.
[178] *Kay*, 2018 WL 3995902, at *2.
[179] *Id*.
[180] United States v. Tuggle, No. 16-cr-20070-JES-JEH, 2018 WL 3631881, at *1 (C.D. Ill. July 31, 2018).
[181] *Id*.

to the public."[182] In denying the defendant's motion to suppress the evidence obtained by the pole cameras, the court stressed that the Supreme Court's extension of Fourth Amendment protections to address surveillance methods implicating new technologies does not apply to "ordinary video cameras that have been around for decades."[183]

These lower court decisions apply a very textualist interpretation of *Carpenter*, excluding security cameras altogether from technologies that merit additional Fourth Amendment protections. However, they may not accurately reflect the framework put forth by *Carpenter*. Although the majority opinion did explicitly state that *Carpenter* does not apply to security cameras,[184] security cameras have developed (and are continuing to develop) far beyond what the Court may have contemplated. For example, improved resolution and zoom capabilities may allow law enforcement officials to learn more details than those learned by analog cameras, such as license plate numbers and identifying features of persons captured by the pole cameras.[185] In one district court case, the simple abilities to "pan and tilt" a camera "from afar" contributed to a judge's decision to suppress evidence obtained from that camera.[186] Additionally, facial-recognition software and LPR cameras are innovations that are either in-use or in-development.[187] Categorizing these advancements as "possible because of the digital age" would be in line with the Supreme Court's application of the Fourth Amendment in *Kyllo*: "While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."[188]

On the other hand, it seems unlikely that innovations to pole cameras qualify as the "seismic shift[]"[189] in technology that generates the unique records the Court envisioned. This seems to be the more likely analysis. While the internet certainly made it easier to access and view recordings in real-time, it did not transform the nature of the pole camera's metadata.[190] The developments to the functionality of pole cameras such as the ability to zoom, day and night capabilities, and twenty-four hour video surveillance do not truly change the nature of what we can learn from watching a video recording. Instead, it really comes down to placement. For example, an officer could learn the same license plate information from an analog video camera placed closer to a vehicle than he could from a zoomed-in pole camera placed further from the vehicle or a pole camera with an LPR camera attachment. Thus, these advancements have simply made video surveillance more efficient; but the records of video footage have remained largely the same as they were prior to the digital age, and they do not "give[] police access to a category of information otherwise unknowable."[191]

---

[182] *Id*.
[183] *Id*. at *3.
[184] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
[185] *See supra* Part V.A.
[186] United States v. Moore-Bush, 381 F.Supp.3d 139, 150 (D. Mass. 2019).
[187] *Id*.
[188] Kyllo v. United States, 533 U.S. 27, 36 (2001).
[189] *Carpenter*, 138 S. Ct. at 2219.
[190] *See* Kerr, *supra* note 3 (manuscript at 46).
[191] *Carpenter*, 138 S. Ct. at 2218.

If courts do ultimately decide that that pole camera innovations were made possible by the digital age, the second prong of the *Carpenter* framework is easily met. Pole camera video footage is collected without any meaningful voluntary choice of the target when pole cameras are installed by law enforcement officials with only the consent of utility companies. Individuals are not given the option to opt out of the video surveillance because the pole cameras are installed with the intention to "build evidence against an alleged individual associated with . . . criminal activity."[192]

The third prong is less clear. The footage can reveal an intimate portrait of a person's life based on what the video captures. For example, recordings of the guests that a person invites into their home can provide insight into their "familial, political, professional, religious, and sexual associations."[193] In tension with most other rulings, the court in *United States v. Moore-Bush* found that pole camera surveillance of people who entered and exited a suspect's home for eight months was a search under *Carpenter*.[194] The court emphasized the "recorded and digitized" nature of pole cameras and that the government can review footage "with to-the-second specificity"[195] to determine that an individual has a reasonable expectation of privacy in the "comings and goings" of their houseguests.[196] Judge Young gave the example that "the Government has no business knowing that someone other than the occupant's spouse visited the home late at night when the spouse was away and left early in the morning" to demonstrate that this long-term tracking does provide an intimate window into a person's life.[197]

On the other hand, according to one Wisconsin district court, pole camera surveillance may not provide the same "*aggregate* account of a person's life" as CSLI.[198] Instead, "[p]ole cameras are limited to a fixed location and capture only activities in camera view, as opposed to GPS, which can track an individual's movement anywhere in the world."[199] This analysis aligns with how courts are generally applying *Carpenter*.[200] In *United States v. Kelly*, the court determined that stationary video surveillance can only capture limited information such as the number of people entering or exiting an apartment, when they entered or exited, and occasionally who the people were.[201] The court rejected "[t]he defendant's attempt to equate a process that records only what someone standing in the apartment hallway, or outside the apartment complex, could have seen with a process [that] [sic] follows a person into homes, places of worship, hotels, bedrooms, restaurants and meetings."[202] Realistically, the footage obtained from such video

---

[192] IRS, *supra* note 140.

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

[194] United States v. Moore-Bush, 381 F.Supp.3d 139, 140 (D. Mass. 2019).

[195] *Id*. at 149.

[196] *Id*. at 143–44.

[197] *Id*. at 148.

[198] United States v. Tirado, No. 16-CR-168, 2018 WL 3995901, at *2 (D. Wis. Aug. 21, 2018) (emphasis added).

[199] United States v. Tuggle, No. 16-CR-20070-JES-JEH, 2018 WL 3631881, at *3 (C.D. Ill. July 31, 2018).

[200] *See, e.g*., United States v. Kelly, 285 F.Supp.3d 721, 726–27 (D. Wis. 2019).

[201] *Id*.

[202] *Id*. at 727.

surveillance cannot possibly track the totality of an individual's movements or provide the same intimate details that can be deduced from CSLI.

Ultimately, courts are unlikely to have to consider the second and third prongs. Because the digital age has not substantially transformed the nature of video surveillance, pole cameras should not qualify for an additional layer of protection under *Carpenter*.

VI. INTERNET PROTOCOL ("IP") ADDRESSES

The third technology addressed in this paper is an Internet Protocol, or IP, address. IP addresses were widely considered by the judicial system prior to *Carpenter*. "Indeed, '[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.'"[203] However, given that IP addresses are a critical component involved with participation in the internet, which is itself such a pervasive part of modern society, it seems possible that they should be classified as a digital age technology worthy of reconsideration.

A. TECHNOLOGY OVERVIEW

At its core, an IP address is a unique number that is assigned to a device that connects to the Internet.[204] Internet Service Providers ("ISPs") "assign IP addresses to their subscribers, logging who is using what address at any given time."[205] The collection of numbers in an IP address indicates a user's network and computer (or host).[206] In the same way that a "home[] has a unique address assigned to it that allows for mail to be received, take-out to be delivered, or emergency services to be directed to it[,]" a unique IP address allows devices to send and receive data from other devices connected

---

[203] United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (quoting United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008)).

[204] ANTHONY T. HOLDENER, III, HTML5 GEOLOCATION 9 (Simon St. Laurent ed., 2011).

[205] Joshua J. McIntyre, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information*, 60 DEPAUL L. REV. 895, 897 (2011). There are both public and private IP addresses; a private IP address exists for each device on a network, which can only be seen by the devices on the local network. Chris Hoffman, *How to Find Your Private and Public IP Addresses*, HOW-TO GEEK (July 3, 2017, 12:22 PM), https://www.howtogeek.com/117371/how-to-find-your-computers-private-public-ip-addresses/. The "ISP assigns a *public* IP address that other devices on the Internet can see." *Id*.

[206] *Why is Your IP Address Broken Into Four Sections?*, WHAT IS MY IP ADDRESS, https://whatismyipaddress.com/ipv4-parts (last visited Mar. 6, 2019). There are two standards for IP addresses: IPv6 and IPv4. Rob Mardisalu, *IPv4 vs. IPv6*, THE BEST VPN (Dec. 11, 2017), https://thebestvpn.com/ipv4-vs-ipv6/. IPv4 addresses were developed in 1983 and are still widely used today. *Id*. IPv4 "uses a 32-bit addressing scheme to support 4.3 billion devices, which was [previously] thought to be enough." Keith Shaw, *What is IPv6, and Why Aren't We There Yet?*, NETWORK WORLD (Sept. 27, 2018, 2:58 PM), https://www.networkworld.com/article/3254575/what-is-ipv6-and-why-aren-t-we-there-yet.html. "However, the growth of the internet, personal computers, smartphones and now Internet of Things devices" led the Internet Engineering Task Force (IETF) to create a new standard, IPv6, in 1998. *Id*. "Most of the world 'ran out' of new IPv4 addresses between 2011 and 2018 – but we won't completely be out of them as IPv4 addresses get sold and re-used." *Id*. IPv6 uses a 128-bit addressing scheme to support approximately 340 trillion devices. *Id*. There is limited data on the accuracy of IPv6 geolocation capabilities. *See* JAN-JELLE KESTER, COMPARING THE ACCURACY OF IPV4 AND IPV6 GEOLOCATION DATABASES 1 (2016), https://pdfs.semanticscholar.org/0705/1014673302f97a762e74b795b70efdd74a1c.pdf?_ga=2.118293825.936373604.1570464840-520238280.1570464840. Therefore, "IP" will be used throughout this paper as a general reference to both protocols but mainly to IPv4.

to the Internet.[207] Unlike an assigned home address, however, IP addresses are not necessarily permanent.[208] Instead, "an IP address may be either *static* (permanent) or *dynamic* (temporary),[209] meaning that a user could have a different IP address each time they log into the internet.

Nearly all IP addresses are dynamic.[210] Dynamic IP addresses constantly change each time a user accesses the internet,[211] making it much more difficult for geolocation services to accurately assess an individual's whereabouts.[212] However, "most ISPs reassign the same address to a subscriber every time he logs on to the network."[213] Therefore, "[e]ven with dynamic addressing, a computer may retain a single IP address assignment for months at a time . . . [, and therefore,] even dynamic IP addresses can be associated with particular individuals."[214] On the other hand, organizations or companies will use Network Address Translation ("NAT"), a "process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network."[215] As a result, the number of public IP addresses used by the organization or company is limited because multiple computers will share the same IP address.[216]

Both ISPs and the websites that a user visits collect and store IP addresses.[217] "It is common for websites to keep a record of all IP addresses that visited with the date and time of the visit."[218] An ISP also maintains a log of individuals' internet activity.[219] "Even if [an] IP address is a dynamic address . . . [the] ISP will be able to identify [a user's] browsing activity because it knows what number was allocated to which customer and when."[220]

Some limited information can then be determined just by knowing the IP address, including a rough estimation of a user's geolocation. During the past twenty years, "'IP Geolocation' emerged as a means of associating IP addresses with physical locations, such as continent, country, state/province (where relevant), and city, as well as . . . ZIP/postal code, area code, time

---

[207] HOLDENER, *supra* note 204, at 9.

[208] *Id*.

[209] *Id*.

[210] *DHCP: The Networking Protocol That Gives You an IP Address*, WHAT IS MY IP ADDRESS, https://whatismyipaddress.com/dhcp (last visited Mar. 6, 2019).

[211] *Id*.

[212] IP Location, *How Accurate is IP-based Geolocation Lookup?*, IP LOCATION (Nov. 17, 2016), https://www.iplocation.net/geolocation-accuracy.

[213] McIntyre, *supra* note 205, at 913. It is important to

note[] that the duration of an IP address assignment can vary from a few days to a few months, depending on a number of factors such as the size of the pool of IP addresses available to the ISP, the number of subscribers and the relative stability of the network.

OFFICE OF THE PRIVACY COMM'R OF CAN., WHAT AN IP ADDRESS CAN REVEAL ABOUT YOU 8 (May 2013), https://www.priv.gc.ca/media/1767/ip_201305_e.pdf.

[214] McIntyre, *supra* note 205, at 913.

[215] *What is Network Address Translation?*, WHAT IS MY IP ADDRESS, https://whatismyipaddress.com/nat (last visited Mar. 6, 2019).

[216] *See id*. Although offices may use a single IP address for numerous colleagues, the office likely "can still identify which computer on its network accessed a particular site." *IP Addresses and the Data Protection Act*, PINSENT MASONS: OUT-LAW (May 2007), https://www.pinsentmasons.com/out-law/guides/ip-addresses-and-the-data-protection-act.

[217] *IP Addresses and the Data Protection Act*, *supra* note 216.

[218] *Id*.

[219] *Id*.

[220] *Id*.

zone, connection type, etc."[221] IP addresses are typically "assigned to an ISP within blocks that are based on region by a local registry institution. Because of this, the country, region, and even city are generally easy to identify for a given IP address."[222] In fact, "[a] device's geographical location can frequently be pinpointed to within a few meters of its actual location" given advancements in ISP data collection capabilities.[223]

The precision with which a device can be located using IP addresses is continuing to grow. In 2011, computer scientists at Northwestern University in Evanston, Illinois and at the University of Electronic Science and Technology of China in Chengdu developed a three-tier methodology that can identify a device using only an IP address with a median error distance of 690 meters.[224] This geolocation technique was "50 times more accurate[] than the best previous system."[225] Overall, however, technology has not advanced to the point where IP addresses can definitively point to a specific user without the assistance of an ISP to determine the residence to which the IP address is registered.

Viewed alone, IP addresses generally do not reveal much personal information about an individual beyond their general location.[226] Nevertheless, "onlookers can in some cases look at the online activity associated with a particular IP address. Then, they can stitch together a lot of information about the people or even a single person who's accessing the internet from that address."[227] In 2013, the Office of the Privacy Commissioner of Canada ("OPC") published a report that examined the privacy implications of various "elements of subscriber information" including IP addresses.[228] Based on the study, the OPC found that "it was possible to build a detailed profile of a person or group associated with the IP address."[229] Specifically, it determined that knowledge of an IP address enables a searcher to "search the Internet using the IP address or computer names. The results of these searches might reveal peer-to-peer ("P2P") activities (e.g., file sharing), records in web server log files, or glimpses of the individual's web activities . . . ."[230]

For example, the OPC conducted a test using "the IP address of the web proxy of the Office of the Privacy Commissioner of Canada. A WHOIS lookup revealed that the IP address was assigned to the Public Works and Government Services ("PWGSC")," as well as the physical address,

---

[221] David Belson, *Finding Yourself: The Challenges of Accurate IP Geolocation*, ORACLE DYN: VANTAGEPOINT (Jan. 29, 2018), https://dyn.com/blog/finding-yourself-the-challenges-of-accurate-ip-geolocation/.

[222] HOLDENER, *supra* note 204, at 9.

[223] *Id*.

[224] Yong Wang et al., *Towards Street-Level Client-Independent IP Geolocation*, NW. NETWORK GROUP PUBLICATIONS 1, 1–2 (2011), http://networks.cs.northwestern.edu/technicalreport.pdf.

[225] *Id*. at 1.

[226] Cale Guthrie Weissman, *What is an IP Address and What Can it Reveal About You?*, BUSINESS INSIDER (May 18, 2015, 1:45 PM), https://www.businessinsider.com/ip-address-what-they-can-reveal-about-you-2015-5.

[227] *Id*.

[228] OFFICE OF THE PRIVACY COMM'R OF CAN., *supra* note 213, at 1.

[229] *Id*. at 2.

[230] *Id*. at 4.

technical point of contact's full name, email address, and phone number.[231] Searching the IP addresses "yielded more than 240 'hits.' The results revealed that individuals working behind the IP address had visited sites dealing with . . . legal advice related to insurance law and personal injury litigation; a specific religious group; fitness . . . and specific entertainers."[232] Importantly, the OPC notes that this data came from looking at "the online activity of a group of computers, not an individual work station."[233]

B. *CARPENTER* APPLICATION

An individual's expectation of privacy in IP addresses has continued to be considered by the courts, often in cases concerning child pornography.[234] However, as with pole cameras, courts have been reluctant to extend the logic of *Carpenter* to IP addresses. For example, in *United States v. Monroe*, the District Court of Rhode Island rejected the defendant's argument that *Carpenter* required the Government to obtain a warrant to compel the disclosure of IP addresses.[235] In this case, law enforcement officials were "investigat[ing] an internet-based bulletin board dedicated to the advertisement, distribution, and production of child pornography."[236] Officials identified "eleven URLs linking to video files depicting child pornography" and were granted orders under 18 U.S.C. §2703(d) compelling the file sharing site ("FSS") that hosted the video files "to disclose, among other records: (1) the IP address of any device that uploaded or downloaded content from the targeted URLs; and (2) the dates and times these files were uploaded or downloaded."[237] From the IP addresses produced in these records, officials were able to use "publicly available search tools" to determine the controlling ISP.[238] In response to subpoenas, the ISP disclosed the address of the subscriber to the assigned IP address and the government was able to investigate the home further to identify the defendant, Jordan Monroe, which led to his subsequent arrest.[239]

Relying on *Carpenter*, Monroe moved to suppress the evidence stemming from the acquisition of his IP address.[240] "The Court [was] unpersuaded, however, that the Government's acquisition of a defendant's historical . . . [CSLI] from a third party [was] analogous to the circumstances here."[241] Instead, the court distinguished these technologies, stating that IP addresses "can only provide 'the location at which one of any number of computer devices may be deployed, much like a telephone number can be

---

[231] *Id*. at 4–5. WHOIS is an IP lookup tool that returns "as much information as possible for a given IP address, sourced from the Regional Internet Registry ("RIR") to which the address belongs. A RIR is an organization that manages the allocation and registration of Internet number resources within a particular region of the world." *WHOIS IP Lookup Tool*, NEUSTAR, https://www.ultratools.com/tools/ipWhoisLookup (last visited Mar. 6, 2019).

[232] *See* OFFICE OF THE PRIVACY COMM'R OF CAN., *supra* note 213, at 5.

[233] *Id*.

[234] *See generally, e.g.*, United States v. Contreras, 905 F.3d 853 (5th Cir. 2018); United States v. Bynum, 604 F.3d 161 (4th Cir. 2010); United States v. Monroe, 350 F. Supp. 3d 43, 44 (D.R.I. 2018).

[235] *Monroe*, 350 F. Supp. 3d at 44.

[236] *Id*.

[237] *Id*. at 45. *See generally* 18 U.S.C. § 2703(d) (2019).

[238] *Monroe*, 350 F. Supp. 3d at 45.

[239] *Id*. at 45–46.

[240] *Id*. at 44.

[241] *Id*. at 48.

used for any number of telephones" and that "[i]t does not, in and of itself, reveal a particular user's identity or the content of the user's communications."[242] Rather, "[a]n IP address is *one* link held by a third party in a chain of information that may lead to a particular person."[243]

On October 1, 2018, the Fifth Circuit came to a similar conclusion in *United States v. Contreras*.[244] Here, the court found that IP addresses "fall[] comfortably within the scope of the third-party doctrine"[245] as traditionally understood because they qualify as "business records that might *incidentally* reveal location information."[246] Because the business records at issue "revealed only that the IP address was associated with the [defendant's] residence[,]" the defendant did not have a reasonable expectation of privacy in this information.[247]

In both of these decisions, the courts made a decision about the extent of information that can be learned from IP addresses. However, advancements in the technology may warrant a different result. First, we consider whether IP addresses are records made possible as a result of the digital age. Under Kerr's framework, "[p]re-digital records and *their modern equivalents* are exempt."[248] We know from *Carpenter* that telephone numbers and bank registers are categorized as the pre-digital records that *Carpenter* did not disturb.[249] An IP address may be an example of technology that is the modern equivalent of a telephone number. Similar to a phone number, an IP address identifies a device by which to communicate with; it is a unique set of numbers that identifies a computer to connect with other computers to send and receive data over a network.[250] Knowing a phone number does not necessarily indicate the person making or receiving a phone call. Similarly, knowing an IP address does not necessarily indicate who is connecting to a network to send and receive data in the absence of further investigation.[251]

On the other hand, the collection of IP addresses could fundamentally be considered an important advancement in the digital age, given the prevalence of the internet in modern society. This, along with improved geolocation tracking, may indicate that IP addresses have the potential to someday reveal the real-time location of users while connected to the Internet. However, this technology is not yet in-use or even in-development. Instead, even the best available geolocation methods can be considerably inaccurate.[252] As the technology currently exists, it does not do more than reveal the general location of an IP address.[253] Again, without additional context, this information is practically meaningless.

---

[242] *Id*.
[243] *Id*. at 49 (emphasis added).
[244] United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018).
[245] *Id*.
[246] *Id*. (emphasis added) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018)).
[247] *Id*.
[248] Kerr, *supra* note 3 (manuscript at 16) (emphasis added).
[249] *Carpenter*, 138 S. Ct. at 2220 (discussing that the opinion does not call into question conventional surveillance techniques).
[250] *See supra* Part VI.A.
[251] *See, e.g.*, United States v. Monroe, 350 F. Supp. 3d 43, 49 (D.R.I. 2018).
[252] *See* Bradley Mitchell, *Does IP Address Location (Geolocation) Really Work?*, LIFEWIRE (Feb. 28, 2020), https://www.lifewire.com/does-ip-address-geolocation-really-work-818154.
[253] *Supra* Part VI.A.

The second requirement of the framework asks whether the records of IP addresses were created without the user's meaningful voluntary choice. This requirement seems easily met. The use of the internet has become "a pervasive and insistent part of daily life[,]"[254] much like using a cell phone. Communicating over the internet is "indispensable to participation in modern society."[255] However, all of our online activity leaves a trail of our IP addresses behind. This is fundamentally what allows us to send and receive data over the internet.[256] Thus, as with CSLI, the only way to avoid creating these records is to avoid engaging in the internet altogether. Opting to use the internet should not amount to a voluntary decision to reveal a user's IP address with third parties. Therefore, this requirement is likely met. The court in *Contreras* argued that IP addresses fall within the scope of the traditional third-party doctrine because they incidentally reveal location information. However, the third-party doctrine focuses on the *voluntariness* of the information revealed, rather than the extent of what can be learned from the information.[257] For this inquiry, we move to the third requirement of the *Carpenter* framework.

The analysis under the third requirement somewhat mirrors the limitations of IP addresses discussed under the first requirement. Because the technology has not been developed to the point where it can provide the same sort of aggregate information as CSLI, it likely fails this prong of the test. An IP address, on its own, does not present any revealing information. Instead, the IP address must be viewed in conjunction with the assigned user's online activity in order to reveal the "privacies of life"[258] that *Carpenter* is aimed at protecting. Although the OPC's study discussed earlier suggests that IP addresses reveal this sort of intimate information, it was not possible to link the online activity to a specific individual.[259] Instead, the OPC could determine the aggregate search history derived from a group of computers.[260] This understanding aligns with the court's reasoning in *Monroe*, where more investigation beyond just obtaining an IP address led law enforcement to the authorities.[261] Government officials had to "determin[e] the internet service provider that owned the IP address, subpoena[] the provider's subscriber information, and conduct[] additional surveillance."[262]

In sum, IP addresses are likely to fail both the first and second requirement of the *Carpenter* framework. Because IP addresses mimic pre-digital age surveillance records, they cannot qualify as a "seismic shift" technology that the Court considered for additional protections. Furthermore, they do not, on their own, reveal the sort of intimate window into a person's life as CSLI does. Therefore, an individual should not have an expectation of privacy in IP address records under *Carpenter*.

---

[254] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
[255] *Id*. (quoting Riley v. United States, 573 U.S. 373 (2014)).
[256] *See supra* Part VI.A.
[257] *See*, *e.g*., Kerr, *supra* note 3 (manuscript at 20).
[258] *Carpenter*, 138 S. Ct. at 2217 (internal quotations omitted).
[259] *See* OFFICE OF THE PRIVACY COMM'R OF CAN., *supra* note 213, at 5.
[260] *Id*.
[261] United States v. Monroe, 350 F. Supp. 3d 43, 49 (D.R.I. 2018).
[262] *Id*.

VII. CONCLUSION

Carpenter changed the way that courts look at technologies under the Fourth Amendment. In the digital age, law enforcement officials are able to rely on vastly more innovative surveillance tactics to promote security. The judicial system, however, needs to be cognizant of balancing the government's interest in security with an individual's expectation of privacy in the technology relied upon. Because there are technologies available that have a tendency to reveal a deeply intimate picture of an individual's life, well-beyond the interests of law enforcement in criminal investigations, we need to protect those technologies from unreasonable searches and seizures.

Under the framework put forth by *Carpenter*, the technologies that merit additional Fourth Amendment protections are ones whose records were made possible because of the digital age, that log records without any meaningful voluntary choice of the user, and that have a tendency to reveal an intimate portrait of a person's life. With this framework in mind, smart meters should qualify for additional protections, but other technologies including pole cameras and IP addresses should not. Pole cameras and IP addresses do not offer a new kind of record made possible by the digital age. However, as these technologies continue to develop at an exponentially rapid pace, they may have to be reexamined again to continue to maintain the balance that underlies our basic Fourth Amendment right to privacy.