GRIN AND “BARE” IT: THE SEVENTH CIRCUIT’S STAMP OF APPROVAL ON UNREASONABLE FOURTH AMENDMENT VIOLATIONS

ASHLEY L. SURINAK*

Cite as: Ashley L. Surinak, Grin and “Bare” It: The Seventh Circuit’s Stamp of Approval on Unreasonable Fourth Amendment Violations, 14 SEVENTH CIRCUIT REV. 98 (2018), at https://www.kentlaw.iit.edu/sites/ck/files/public/academics/jd/7cr/v14/surinak.pdf.

INTRODUCTION

When is a person’s expectation of privacy “reasonable?” In 1967, the Supreme Court held that an electronic listening recording device atop a public telephone booth was an unreasonable invasion of privacy.1 Conversely, in 1979, the Court deemed a pen register (an electronic device that records dialed phone numbers from a particular line) on phone company property reasonable.2 In 2001 and 2012, respectively, the Court reasoned that the use of an Agema Thermovision 210 thermal imaging device to detect rudimentary heat registers of a home was unreasonable,3 as was the use of a global-positioning-system (GPS) tracking device to chart an individual’s

* J.D. candidate, May 2019, Chicago-Kent of Law College, Illinois Institute of Technology. Executive Articles Editor, Chicago-Kent Law Review. Thank you to Lawrence Surinak for his constant support, legal insight, and willingness to discuss the Fourth Amendment after work hours. A special thanks to Stacey Surinak as well, my Naperville-based field researcher who spoke to any utility providers she caught at the source.

movements for twenty-eight days. And in 2018, the Supreme Court found that 127 days of cell-site location data (CSLI), obtained without a warrant, was unreasonable, too.

Determining reasonability is at the heart of Fourth Amendment analysis. Specifically, courts must ask: (1) whether an individual has exhibited an actual, subjective expectation of privacy; and (2) whether this expectation is one that society would recognize as being “reasonable.” Courts reject mechanical Fourth Amendment interpretations in favor of an approach that lends generous support to citizen privacy. Doing so ensures that no individual is “at the mercy of advancing technology.” Indeed, courts are bound to “take account of more sophisticated systems that are already in use or in development.” Undoubtedly, the most pressing Fourth Amendment issue to arise in the advent of new technology is how information is obtained. This issue touches on the second part of the Fourth Amendment analysis: reasonability. Information is typically obtained by one of two means: a (1) court order; or (2) warrant. The most marked difference between the two is the standard that must be met. For example, a court order granted pursuant to the Stored Communications Act requires a showing of “reasonable grounds” for believing that records were “relevant and material to an ongoing investigation.” In contrast, a warrant requires probable cause, which is a significantly heightened standard from “reasonable grounds.” Courts have historically held that official intrusion into the private sphere, in violation of the Fourth Amendment, generally requires a warrant supported by probable

---

6 Katz, 389 U.S. at 361 (Harlan, J., concurring).
7 Kyllo, 533 U.S. at 35.
8 Id.
9 Id. at 36.
11 Carpenter, 138 S. Ct. at 2221.
cause.\(^{12}\) In the Fourth Amendment context, this difference is marked, though in other areas of law the terms are used almost synonymously.\(^{13}\)

In *Naperville Smart Meter Awareness v. City of Naperville*, the Seventh Circuit held that, although the City of Naperville conducted a Fourth Amendment search when it replaced analog energy meters with digital “smart meters,” Naperville residents did not have a reasonable expectation of privacy in the data the meters produced.\(^{14}\) Thus, the City of Naperville can now compile the smart meter data – every fifteen minutes – without a warrant and store it for up to three years.\(^{15}\) The Seventh Circuit set forth a cautionary posture, clarifying that decisions such as this are case-dependent and may vary due to factors such as the interval of data collection or accessibility of data to law enforcement.\(^{16}\) Yet, because smart meters allow for more efficient power restoration, reduce strain on the power grid, and lessen labor costs, the court found that the fifteen-minute data collection intervals were reasonable.\(^{17}\)

This comment will argue that the Seventh Circuit erred in rejecting the plaintiff’s request to file a third amended complaint and that any “balancing test” to determine the “reasonable” component of a Fourth Amendment inquiry is untenable and unconstitutional under strict scrutiny analysis. These issues are particularly pressing in consideration of technological advancement’s rapid pace. While reasonability may be context-specific, the precedent the Seventh Circuit established here is dangerous because it was made without considering the ramifications of massive data collection, regardless of the context of that collection. This comment will also argue that


\(^{13}\) *See, e.g.*, 625 ILL. COMP. STAT. ANN. 5/2-118.1(b)(2) (West, Westlaw through P.A. 110-1114); *People v. Fortney*, 297 Ill. App. 3d 79, 87 (2d Dist. 1998) (citing *People v. Brodeur*, 189 Ill. App. 3d 936, 940 (2d Dist. 1989)).

\(^{14}\) *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 524 (7th Cir. 2018).

\(^{15}\) *Id.* at 524.

\(^{16}\) *Id.* at 529.

\(^{17}\) *Id.*
defining distinct categories as to what is reasonable or unreasonable is an equally poor solution, as has been noted by other courts considering the matter.\textsuperscript{18}

The Supreme Court, in accordance with \textit{Smith v. Maryland} and \textit{United States v. Miller},\textsuperscript{19} generally employs a quasi-balancing test to weigh each party’s respective interests in various types of information. This method forces courts to give credence to the “quality or quantity of information obtained” in a search, which has never been tied to the Fourth Amendment’s protections, whether in the home or elsewhere.\textsuperscript{20} By making determinations as to what is protected in the home, including the nature of what is protected in the home based upon the intervals at which the data is collected, the Seventh Circuit compromised the Fourth Amendment protections the framers intended.\textsuperscript{21} The third-party doctrine is inapplicable where the City of Naperville required the installation of digital smart meters to replace the analog meters because the City is the only electric provider, further heightening the risk of private information disclosure.\textsuperscript{22} Plainly put, residents were given no choice in this matter, and the repercussions of the Seventh Circuit’s ruling, against the will of the City of Naperville’s citizens, should not be taken lightly.

Section I of this comment will discuss the historical underpinnings of the Fourth Amendment, along with its protections as technology has continued to advance. Section II will discuss the background of \textit{Naperville Smart Meter Awareness v. City of Naperville}, and how the Seventh Circuit reached its decision to deny the plaintiff’s request to file a third amended complaint. Section III

\begin{footnotesize}
\textsuperscript{18} Kyllo v. United States, 533 U.S. 27, 41-51 (2001). (Stevens, J., dissenting) (positing that the balancing test is a misinterpretation of \textit{Smith v. Maryland} and \textit{United States v. Miller}, as are suggestions to establish distinct categories of information that require a warrant and those that do not).


\textsuperscript{20} \textit{Kyllo}, 533 U.S. at 27.

\textsuperscript{21} See infra notes 28-41.

\textsuperscript{22} Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 526–27 (7th Cir. 2018).
\end{footnotesize}
will discuss why the Seventh Circuit erred by reviewing precedent and policy considerations. Section III will also reveal why all courts, the Seventh Circuit included, should proceed with Fourth Amendment analysis on a case-by-case basis to safeguard constitutional privacy guarantees pursuant to strict scrutiny analysis.

I. THE FOURTH AMENDMENT

The Fourth Amendment guarantees “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”23 This right “shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”24 But, when is a search a “search?” And when is a search “unreasonable?”

Technological advancements have inarguably changed the purview of the Fourth Amendment’s reach, and in a confusing way. But, how did the courts arrive at this juncture? Traditionally, the Fourth Amendment applied to property interests by protecting against trespass.25 However, courts expanded this application to hold that the “principal” object of the Fourth Amendment is not the protection of property, but of privacy.26 This shift came about from judicial recognition that privacy should be protected from unreasonable invasions.27 Today, courts agree about the general test to apply to Fourth Amendment questions,28 but there is no obvious answer to when something is “reasonable.” This is especially true as technology continues to evolve, and at ever-increasing speeds.

23 U.S. CONST. amend. IV.
24 Id.
27 Warden, 387 U.S. at 305.
A. History, Interpretations, and Technological Challenges

The fundamental purpose of the Fourth Amendment “is to safeguard the privacy and security of individuals against arbitrary invasions by government officials.” When it was enacted, the Fourth Amendment was in “response to the reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.” As technology advanced and the government gained access to areas traditionally concealed, particularly within the home, courts struggled to consistently and predictably “assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.” However, despite this ongoing struggle for uniform applicability, the Fourth Amendment unequivocally preserves privacy against the “uninvited ear” of governmental intrusion.

It is critical to understand the meaning of the term “search” for Fourth Amendment interpretation. While the Supreme Court has never adopted an official definition of the term, a search is generally understood as “some exploratory investigation, or an invasion and quest, a looking for or seeking out.” “A search implies a prying into hidden places for that which is concealed and that the object searched for has been hidden or intentionally put out of the way.” Generally speaking, looking at an area open to the public is not a “search.”

32 People v. Richardson, 60 Ill. 2d 189 (1975); People v. Loveless, 80 Ill. App. 3d 1052 (3d Dist. 1980).
34 LAFAVE, supra note 33.
35 Id.
person only has a justified expectation of privacy with respect to the interior of his personal residence.\textsuperscript{36} However, what constitutes a “search” is fact-dependent in each case.

There are two approaches to Fourth Amendment protections: (1) a property-based approach; and (2) a privacy-based approach.\textsuperscript{37} The property-based approach is the traditional approach premised on trespass, which recognizes a privacy interest when the government physically intrudes on a person’s house, papers, or effects.\textsuperscript{38} In contrast, the privacy-based approach is the more modern trend where courts recognize that the Fourth Amendment extends beyond property rights and into other areas in which an individual has a reasonable expectation of privacy.\textsuperscript{39} In the modern approach, courts must ask “whether the complaining person had a reasonable expectation of privacy in the area invaded.”\textsuperscript{40} The privacy-based approach does not detract from the property-based approach;\textsuperscript{41} rather, it provides additional protections.\textsuperscript{42}

The most immediate issue facing courts today in the Fourth Amendment context is technology. After all, the Supreme Court has noted that one cannot mechanically interpret the Fourth Amendment because doing so would “leave the homeowner at the mercy of advancing technology.”\textsuperscript{43} Courts note that while some systems might be crude, the rule the Court adopts has to take account of sophisticated systems already in use or development.\textsuperscript{44} For example, in \textit{Kyllo v. United States}, the Court found that the thermal imager used to scan a

\begin{thebibliography}{9}
\bibitem{const Amend IV} U.S. Const. amend. IV.
\bibitem{Bonilla 2017} People v. Bonilla, 2017 IL App (3d) 160457, ¶ 12.
\bibitem{Jardines} Id. (citing Florida v. Jardines, 569 U.S. 1, 5 (2013)).
\bibitem{Jardines} Bonilla, 2017 IL App (3d) 160457, ¶ 13 (citing Jardines, 569 U.S. at 5–6).
\bibitem{Burns} Bonilla, 2017 IL App (3d) 160457, ¶ 13 (citing Jardines, 569 U.S. at 10–11; People v. Burns, 2016 IL 118973, ¶¶ 27, 45).
\bibitem{Sotomayor} Bonilla, 2017 IL App (3d) 160457, ¶ 13.
\bibitem{United States} Id. at 38.
\end{thebibliography}
triplex, which displayed heat signatures in black (cool), white (hot), and shades of gray for everything in-between, may have been rudimentary, but was technology that nevertheless demanded Fourth Amendment protections.\footnote{Id. at 29–30.} Use of even a rudimentary thermal imager still constituted a “search” in need of protection.\footnote{See infra notes 66–73.} The Court reiterated this concept – that even rudimentary technology is technology that demands constitutional protection – on numerous occasions. Indeed, as Justice Brandeis noted in his dissent in \textit{Olmstead v. United States},\footnote{See infra notes 66–73.} this Court is obligated as “[subtler] and more far-reaching means of invading privacy have become available to the Government,” to ensure that no scientific progress erodes Fourth Amendment protections.\footnote{Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (quoting \textit{Olmstead v. United States}, 277 U.S. 438, 473–74 (1928)).}

\textbf{B. Supreme Court Precedent}

In 1967, the Supreme Court decided \textit{Katz v. United States}.\footnote{Katz v. United States, 389 U.S. 347 (1967).} The \textit{Katz} Court held that Katz had a reasonable expectation of privacy in his communications in a phone booth and that the government, in electronically listening to and recording the conversation, made a “search and seizure” pursuant to the Fourth Amendment.\footnote{Id.} In \textit{Katz}, the Federal Bureau of Investigations (“FBI”) attached an electronic listening and recording device atop a public telephone booth where Katz placed calls.\footnote{Id. at 348.} While the government argued that a public telephone booth is not a constitutionally protected area, the Court, setting forth that the Fourth Amendment protects people, and not places, determined that the location of the calls was immaterial.\footnote{Id. at 351.} Pursuant to the plain language of the Fourth Amendment, location is irrelevant to the protections granted with the exception that people are
always to be secure in their houses. Moreover, due to the privacy-based shift in Fourth Amendment interpretation, it extended to “the recording of oral statements overheard without any ‘technical trespass under . . . local property law.’” Whether a trespass occurred was irrelevant, and the Court found that there was an intrusion into a “constitutionally protected area.”

Almost a decade later, the Court decided United States v. Miller. Miller charged the Court with determining whether a bank depositor had a protectable Fourth Amendment interest in his bank records. The Court found that the bank depositor did not have a reasonable expectation of privacy in bank records, here consisting of microfilms, checks, and deposit slips, because they were not “private papers.” Instead, they were business records. This case addressed third-party doctrine as well, finding that the Fourth Amendment does not prohibit obtaining information that has been revealed to a third party. Here, the depositor assumed the risk that the information would be conveyed to the Government by revealing that information to another entity. Any subpoenas issued to the bank to obtain the depositor’s records, therefore, posed no threat to the depositor’s Fourth Amendment rights.

Later, in Smith v. Maryland, the Court determined whether installation and use of a pen register at the phone company’s central office to record numbers dialed from the petitioner’s home phone

52 U.S. CONST. amend. IV.
54 Silverman, 365 U.S. at 511–12.
56 Id.
57 Id.
58 Id.
60 Miller, 425 U.S. at 443 (citing White, 401 U.S. at 751–52).
61 Miller, 425 U.S. at 444.
constituted a “search” within the meaning of the Fourth Amendment. The Court reasoned that not only is it doubtful that phone users have an expectation of privacy in numbers dialed, but that because the pen register was installed on phone company property, the plaintiff could not claim that any of his property was invaded or that there was an intrusion into a “constitutionally protected area.” The Court reasoned that individuals know that phone companies generally keep records of numbers dialed, especially because at least some of these numbers dialed are set forth on monthly bills. Therefore, there was no reason to expect that numbers would not be recorded. Thus, the actions were not even considered a “search,” and the records were available without a warrant.

_Kylo v. United States_ stands for the proposition that where the government uses a device not in general public use to explore the details of a home “unknowable without physical intrusion,” the surveillance is a “search” and is presumptively “unreasonable” without a warrant. This is pertinent for _Naperville Smart Meter Awareness_ because it involved a home invasion in the context of advancing technology. Agents used a thermal-imaging device to scan Kylo’s triplex to determine whether the heat emanating from it was consistent with lamps generally used for indoor marijuana growth. Both the majority and dissent set forth a proposed standard as to “whether the technology offers the functional equivalent of actual presence in the area being searched.” However, the majority specifically focused on

63 Id.
64 Id. at 741.
65 Id. at 745.
66 Id.
67 Id. at 745–46.
69 Id. at 27.
70 Id. at 39.
retaining the Fourth Amendment’s original meaning. The Court did so by holding that the government conducts a “search” when it uses a device not in general public use to explore details of a home that would otherwise be unknowable, which is presumptively unreasonable without a warrant. The dissent notably determined that, because the infrared camera passively measured heat emitted from a home’s exterior surfaces, the plaintiff could not have a reasonable expectation of privacy in that information. This “through-the-wall” theory of what constitutes a search suggested that anything leaving the home, like an aroma, would not be a search, nor would it be reasonable for an individual to expect this fact to remain private. The dissent likewise expressed concern with the majority’s characterization of whether something is “in general public use,” a factor that disappears once the technology breaches the public sphere.

In 2012, the Supreme Court held that installation of the global positioning system (“GPS”) tracking device on the plaintiff’s Jeep monitoring the vehicle’s movements was a Fourth Amendment “search.” Jones was in possession of his Jeep at all times, and the agents, although legally authorized to install a tracking device on the vehicle within ten days of issuance while the vehicle was located in the District of Columbia, installed the device on the vehicle on the eleventh day, and in Maryland. Justice Alito, concurring, specifically noted that it was the successful functioning of the GPS device that constituted a search and not the placement of the GPS device itself. It is worth noting that United States v. Jones overturned United States

---

71 Id. at 40 (stating that the Fourth Amendment “is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted” (quoting Carroll v. United States, 267 U.S. 132, 149 (1925))).
72 Kyllo, 533 U.S. at 27.
73 Id. at 41 (Stevens, J., dissenting).
74 Id. at 43–44.
75 Id. at 47.
77 Id. at 402–03.
78 Id. at 420–21 (Alito, J., concurring).
v. Garcia. In Garcia, the Seventh Circuit held that, where police attached a GPS tracking device to a suspect’s car, doing so was not a search, nor was it a seizure of the car. The Seventh Circuit held that it was not a seizure because the device did not affect the car’s driving qualities, draw energy from the car, or otherwise “seize” anything from the car. The Seventh Circuit also held that the GPS placement was not a search because the GPS was merely a substitute for a public activity: following a car on a public street. However, the Jones Court found that the car was an “effect” within the meaning of the Fourth Amendment, and the warrantless GPS placement on the Jeep was a physical intrusion that violated the Fourth Amendment.

In its most recent interpretation of the Fourth Amendment, the Court analyzed two overlapping lines of cases; those that implicate a person’s expectation of privacy in: (1) physical location; and (2) information voluntarily turned over to third parties. In Carpenter v. United States, wireless carriers produced cell-site location information (“CSLI”), providing the government with 12,898 location points that catalogued Carpenter’s movements over 127 days. The government obtained this information via court orders pursuant to the Stored Communications Act after setting forth “specific and articulable facts showing that there are reasonable grounds to believe” that the records sought “are relevant and material to an ongoing criminal

79 474 F.3d 994 (7th Cir. 2007).
80 Id. at 996–97.
81 Id. at 996.
82 Id. at 997.
85 See generally Jones, 565 U.S. at 400.
86 See United States v. Miller, 425 U.S. 435 (1976) (finding there is no expectation of privacy in financial records held by a bank); Smith v. Maryland, 442 U.S. 735 (1979) (finding there is no expectation of privacy in the records of dialed telephone numbers conveyed to a telephone company).
87 Carpenter, 138 S. Ct. at 2209.
The government used the information to produce maps placing Carpenter’s phone near four of the charged robbery locations. The Court of Appeals for the Sixth Circuit affirmed the district court, holding that Carpenter lacked a reasonable expectation of privacy in the information given to the FBI because he had voluntarily shared that information with his cell phone provider, a third party.

The Carpenter Court likened the CSLI data to GPS data, like that at issue in Jones, because in both instances, it is “detailed, encyclopedic, and effortlessly compiled.” However, the Carpenter Court found that the CSLI data was of greater concern than the GPS data because CSLI data involves “the individual continuously reveal[ing] his location to his wireless carrier.” A defendant traveling over public streets may “voluntarily convey[] to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction.” In United States v. Knotts, the government used a beeper merely to assist in tracking a vehicle that was also being followed via air search. However, Knotts was in contrast to Carpenter because the CSLI data collected was the only means used to track Carpenter. The movements in Knotts were on public roads, and the beeper was placed to assist law enforcement in tracking the movements, and on a short-term basis. Carpenter “is not about ‘using a phone’ or a person’s movement at a particular time,” but is “about a detailed chronicle of a person’s physical presence compiled

88 Id. at 2212.
89 Id. at 2212–13.
90 Id. at 2213.
91 Id. at 2216.
92 Id.
94 Id.
96 Knotts, 460 U.S. at 284–85.
every day.” Thus, the privacy concerns at issue in *Carpenter* are greater than those in *Smith* or *Miller*.

The Court took greater concern with the proposition that CSLI is “shared” with the wireless carrier within the meaning of the third-party doctrine. Specifically, the Court found that CSLI is not shared like typical information because cell phones and their services are “such a pervasive and insistent part of daily life” that carrying one is “indispensable to participation in modern society.” There is no “affirmative act” a user takes to share information with a cellular provider; powering up means that sharing is constant and the phone will automatically generate CSLI based on calls, texts, e-mails, and other data connections. Thus, a person’s “options” are to (1) disconnect a phone from the network, or (2) to “unvoluntarily” leave a trail of location data. For these reasons, and what can only be considered as Carpenter’s “unvoluntarily” shared data trail, the Court declined to extend the third-party doctrine principles behind *Smith* and *Miller* to *Carpenter*.

It is important to note that *Carpenter* is a narrow decision. *Smith* and *Miller* remain good law, and the *Carpenter* decision is not intended to “call into question conventional surveillance techniques and tools, such as surveillance cameras.” Moreover, because CSLI is “an entirely different species of business record” because it “implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers,” a warrant theoretically would have been required to obtain

---

97 *Carpenter*, 138 S. Ct. at 2220.
98 *Id.*
99 *Id.*
100 *Id.* (quoting *Riley v. United States*, 134 S. Ct. 2473, 2484 (2014)).
101 *Carpenter*, 138 S. Ct. at 2220.
102 *Id.*
103 *Id.*
104 *Id.*
105 *Id.*
the CSLI in this matter. The Court set forth that “[i]f the third-party doctrine does not apply to the ‘modern-day equivalents of an individual’s own “papers” or “effects,”’ then the clear implication is that the documents should receive full Fourth Amendment protection. Notably, there are case-specific exceptions to the warrantless search of an individual’s CSLI, such as when there is a need to pursue a fleeing suspect. Summarily, the Court declined to grant the state unrestricted access to CSLI due to its revealing “depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection.” The third-party doctrine has no bearing on whether the records in Naperville Smart Meter Awareness deserved Fourth Amendment protection because there is no third party.

From the Katz decision in 1967 to the Carpenter decision in 2018, two, vital Fourth Amendment frameworks of analysis hold true. The first is that location is relevant to the extent that there was a trespass. In Smith, the Court considered placement of the pen register tap to rule out trespass, specifically considering whether the citizen’s “‘property’ was invaded or [whether] police intruded into a ‘constitutionally protected area.’” The Smith Court then clarified the distinction between the property-based Fourth Amendment right and a privacy-based right, distinguishing that the issue is whether the government infringed “a legitimate expectation of privacy.” The court aptly referred to this as the Katz analysis, and rightfully so: it was the first of a long line of cases that would further distinguish property- and privacy-based Fourth Amendment rights. The second framework is that the Fourth Amendment protects people, not places. The Katz Court did not consider it dispositive where a phone conversation

106 Id. at 2222.
107 Id.
108 Id. at 2223.
109 Id.
111 Id.
112 Id.
occurred; it only mattered that the conversation occurred and that it was recorded. That was because “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.” Again, this rendered location irrelevant for a privacy-based interest because a person may knowingly expose something to the public in his home – an area explicitly protected by the Fourth Amendment – meaning that anything knowingly revealed could not reasonably be expected to remain private.

II. *NAPERVILLE SMART METER AWARENESS*

In *Naperville Smart Meter Awareness*, the Seventh Circuit determined whether the City of Naperville’s data collection from the electric public utility – which collected data in fifteen-minute intervals – was reasonable under the Fourth Amendment of the United States Constitution and Article I, § 6 of the Illinois Constitution. The City of Naperville, without the consent of its citizens, installed digital “smart meters” to replace traditional, analog meters on all residences to upgrade its power grid. Smart meters show the amount of electricity being used and when it is used. This can reveal information about what is happening inside the home, including energy-consumption patterns. With this information, and the growing catalogue of appliance load signatures, researchers can predict which appliances are present in a home and when they are

---

114 *Id.* (deeming it unimportant that the conversation at issue occurred in a “public” area (the telephone booth) and that it is irrelevant, for Fourth Amendment purposes, as to where certain activities took place).

115 *Katz*, 389 U.S. at 347.

116 *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 524–25 (7th Cir. 2018).

117 *Id.* at 524.

118 *Id.*

119 *Id.* (citing Rashed Mohassel et al., *A Survey on Advanced Metering Infrastructure*, 63 INT’L J. ELECTRICAL POWER & ENERGY SYS. 473, 478 (2014)).
The accuracy and nature of predictions depend on how often data is collected, as well as the sophistication of the technology used to analyze this data.\(^\text{120}\) Data from the meters is stored for up to three years.\(^\text{122}\)

Naperville Smart Meter Awareness is a citizens’ group that brought suit over concern that the meters revealed intimate details of citizens within their homes, such as when they are home, sleeping and eating routines, and what is kept and used in the home and when.\(^\text{123}\) The Seventh Circuit held that the data collected was a search even though it was necessary to draw inferences from the data to determine any personal information about what was actually occurring in a home.\(^\text{124}\) The Seventh Circuit likened the search to that in *Kyllo*, where officials drew inferences from the home’s thermal energy to conclude that special lamps that grow marijuana were being used.\(^\text{125}\) However, the Seventh Circuit noted that the smart meter issue is more invasive than rudimentary thermal images, supporting its finding that collection of the data was a search.\(^\text{126}\)

Although the Seventh Circuit found, without hesitation, that the smart meter data collection was a search, it deemed this search reasonable.\(^\text{127}\) The court partly based its’ opinion on the City of Naperville’s amended “Smart Grid Customer Bill of Rights,” which specifies that without a warrant or court order, the public utility may not provide customer information to third parties.\(^\text{128}\) The third-party doctrine establishes that individuals have reduced expectations of

\(^{120}\) *Naperville Smart Meter Awareness*, 900 F.3d at 524 (citing 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)).

\(^{121}\) *Naperville Smart Meter Awareness*, 900 F.3d at 524.

\(^{122}\) *Id.*

\(^{123}\) *Id.*

\(^{124}\) *Id.* at 526–27.

\(^{125}\) *Id.*

\(^{126}\) *Id.* at 527.

\(^{127}\) *Id.* at 527–29.

\(^{128}\) *Id.* at 528.
privacy “in information knowingly shared with another.” The City of Naperville argued that by entering into a “voluntary” relationship to purchase electricity from the city, citizens sacrificed any expectation of privacy in smart meter data. The Seventh Circuit was not persuaded by this argument, and found that because the City of Naperville provides electricity through its public utility, there was no third party involved.

Because energy usage itself is not a crime, the court deemed the privacy interests in question in Naperville Smart Meter Awareness to be more insignificant than they are in cases where regulatory law violations are criminally enforced. The court found that the government’s interest in the data collection was substantial, where “the modernization of the electrical grid is a priority for both Naperville . . . and the federal government,” as it allows “utilities to restore service more quickly,” “offer[s] time-based pricing” by reducing strain on the grid, and reduces the utilities’ labor costs.

Notably, the Seventh Circuit included a cautionary note immediately preceding its conclusion. The court advised that its holding was dependent on the particular circumstances of the case before it, stating that its conclusion might change “[w]ere a city to collect the data at shorter intervals” or “if the data was more easily accessible to law enforcement or other city officials outside the utility.” Thus, while there was no doubt that this information was a search, the “government interests in the program, and the diminished privacy interests at stake” rendered the search wholly reasonable without a warrant.

---

130 Naperville Smart Meter Awareness, 900 F.3d at 527.
131 Id.
132 Id. at 528 (finding that the warrantless search of private property is “unreasonable” and that the resident had a right to deny warrantless entry by the inspector (discussing Camara v. Mun. Court of S.F., 387 U.S. 523, 530 (1967))).
133 Naperville Smart Meter Awareness, 900 F.3d at 528–29.
134 Id. at 29.
135 Id.
III. SEVENTH CIRCUIT COMPLICATIONS

During oral argument in Carpenter, Nathan Freed Wessler (“Mr. Wessler”) of the American Civil Liberties Union noted the lower courts’ struggle to apply Miller and Smith to sensitive, digital age records.136 Specifically, Mr. Wessler noted that the five courts of appeals are “virtually begging [the Supreme] Court to provide guidance for how to protect these sensitive, digital records that the Court simply could not have imagined four decades ago.”137 Mr. Wessler continued, proposing that certain types of information, “like heart rate data from a smart watch, or fertility tracking data from a smartphone app, information about the interior of a home, for example, from a smart thermostat that knows when the homeowner is at home and perhaps what room they’re in,” could be categorized into records that either are or are not protected.138 Thus, Mr. Wessler proposed that it is consistent with the role of the lower courts to take an interpretative principle from the Supreme Court and apply it over time.139

The Seventh Circuit’s landmark decision in Naperville Smart Meter Awareness is precedential in the Seventh Circuit, and other circuits have yet to decide similar issues. After all, in 2016 alone, electric utilities in the United States had about 70.8 million advanced (smart) meter installations, about 88 percent of which were residential consumer installations.140 Experts predict smart meter installation across the United States will reach 90 million by 2020.141 Thus,

137 Id.
138 Id.
139 Id.
precedent established before more widespread smart meter dissemination will be of great importance in coming years. This is especially true where law enforcement will presumably turn to this technology for investigative purposes, most likely when it is in “general public use.” The Seventh Circuit’s decision, specifically in the government interest balancing analysis, is dangerous, if not detrimental, to this vital precedent. The Seventh Circuit’s reasoning plainly ignores constitutional commands to apply strict scrutiny where a fundamental right is concerned, too. This arbitrary analysis, coupled with the potential, virtually unlimited uses for smart meter data in law enforcement, highlights the dangers lurking in the Seventh Circuit’s Naperville Smart Meter Awareness decision.

A. Precedential History

“The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained.” By way of example, the Supreme Court has held that the physical invasion of the home, “by even a fraction of an inch,” is too much. All details are intimate details in a home, “because the entire area is kept safe from prying government eyes.” Thus, any details of the home are intimate details, regardless of where or the degree to which they are detected. As was set forth in greater detail above, Fourth Amendment protections do not apply where intimate details are readily observable to the public. For example, when a person travels


143 Id. at 37.
145 Kyllo, 533 U.S. at 37.
146 See United States v. Karo, 468 U.S. 705, 735 (1984) (finding that a “search” began when Karo brought the can of ether into his home as it was “concealed from view”); Arizona v. Hicks, 480 U.S. 321 (1987) (finding a search where the officers searched for the serial number on stereo equipment in “plain view” in the alleged suspect’s home).
on a public road, and those movements are available without any technology or surveillance, there is no reasonable expectation of privacy in those movements.\textsuperscript{147} If a person knowingly exposes something in the home to the public, even though the Fourth Amendment explicitly protects the home, there is no reasonable expectation of privacy in those items or effects, either.\textsuperscript{148}

It is dangerous to propose any bright line, categorical rule of what constitutes an “unreasonable” search based on discrete categories of information. After all, the Court has historically, and repeatedly, held that a search is a search when it reveals any details within the home.\textsuperscript{149} This is even more precarious when one considers the rapidly advancing nature of technology. Even at a foundational level, there is no necessary connection between what is “intimate” and “the sophistication of surveillance equipment.”\textsuperscript{150} On point with Naperville Smart Meter Awareness is the Supreme Court’s prior finding that it is insignificant – in terms of the intimacy of information – whether technology reveals “what hour each night the lady of the house takes her daily sauna and bath” or “nothing more intimate than the fact that someone left a closet light on.”\textsuperscript{151} Undoubtedly, courts will differ in what they subjectively find to be “intimate.”\textsuperscript{152} Therefore, so will those courts’ findings as to what is considered the reasonable subject of a search, which may or may not be permissible without a warrant. Such subjectivity is dangerous, especially when new technology reveals increasingly precise data beyond a mere light being left on.\textsuperscript{153}

Mr. Wessler’s suggestion that certain data – especially information from a smart thermostat – can be placed in a discrete

\textsuperscript{147} United States v. Knotts, 460 U.S. 276, 281 (1983) (“A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”).


\textsuperscript{149} See supra notes 68-75.

\textsuperscript{150} Kyllo, 533 U.S. at 38.

\textsuperscript{151} Id. at 38–39.

\textsuperscript{152} Id. at 38.

\textsuperscript{153} Id.
category is shortsighted.\textsuperscript{154} Information from a thermostat is information from within a home that would not otherwise be known to anyone outside of the home without a search. Naperville Smart Meter Awareness raises analogous issues. Smart meters can record data in a range of intervals, but those in the City of Naperville record information every fifteen minutes.\textsuperscript{155} The information can reveal not only what is left on in a home, such as a closet light, but may also uncover other details within a home that would otherwise remain anonymous.\textsuperscript{156} To qualify the City of Naperville’s residents’ Fourth Amendment rights with a “government interest analysis” in light of the “particular circumstances of this case” contradicts precedent, violates mandated constitutional standards of review (strict scrutiny), and establishes dangerous precedent for the judiciary moving forward.\textsuperscript{157}

\textbf{B. Policy Implications}

The Carpenter Court grappled with a person’s expectation of privacy in today’s digital age.\textsuperscript{158} Ultimately, the Carpenter Court declined to extend Smith and Miller to cell site location data.\textsuperscript{159} It did so because of the “unique nature of cell phone location records,” finding Smith and Miller inapplicable regardless of “[w]hether the Government employs its own surveillance technology, as in Jones, or leverages the technology of a wireless carrier.”\textsuperscript{160} Cell phone records contain the “privacies of life,”\textsuperscript{161} and tracking is “remarkably easy,

\textsuperscript{154} See supra note 138.
\textsuperscript{155} Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 524 (7th Cir. 2018).
\textsuperscript{156} Kyllo v. United States, 533 U.S. 27 (2001).
\textsuperscript{158} Id.
\textsuperscript{159} Carpenter, 138 S. Ct. at 2217.
\textsuperscript{160} Id.
\textsuperscript{161} Riley v. California, 134 S. Ct. 2473, 2495 (2014) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).
cheap, and efficient compared to traditional investigative tools.” Further, and analogous to GPS information, “the time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’”

*Carpenter* specifically implicated the third-party doctrine first set forth in *Smith* and *Miller*. *Smith* and *Miller* held that individuals lack “any protected Fourth Amendment interests in records that are possessed, owned, and controlled by a third party.” The *Carpenter* Court declined to extend the third-party doctrine to the CSLI records, finding that, in the “rare case where the suspect has a legitimate privacy interest in records held by a third party,” a warrant is required for a “reasonable” search. The *Carpenter* Court furthered this in stating that “[i]f the third-party doctrine does not apply to the ‘modern-day equivalents of an individual’s own “papers” or “effects,”’ then the clear implication is that the documents should receive full Fourth Amendment protection.” Indeed, the *Jones* Court, just years ago in 2012, reconsidered the premise that an individual has no reasonable expectation of privacy in voluntarily disclosed information. The Court found this approach ill-suited to the digital age, “in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.” This includes disclosure to online retailers of something as simple as the “books, groceries, and medications” that

165. *Id.* at 2260 (Kennedy, J., dissenting).
166. *Id.* at 2211 (majority opinion).
167. *Id.*
individuals purchase. Notably, the court addresses Justice Alito’s point regarding how some may find the “tradeoff” of privacy for convenience “worthwhile” or that the decrease in privacy is simply “inevitable.” Yet, the Court found that sharing information, no matter how mundane, simply by using a phone or the Internet, does not render a search of that information reasonable. Thus, much of the debate regarding modern applications of third-party doctrine, though not directly at issue in Carpenter, is policy-focused on what level of privacy is expected in today’s society.

To that end, the Jones Court specifically suggested that if change is warranted, it should come from the judicial branch. Technology changes dramatically over time. Because of this, the Court found that “[a] legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.” The same can be said about smart meter technology. The smart meter movement is rapidly growing. As more Americans are affected by the technology, and the technology becomes increasingly sophisticated and intrusive, attitudes as to what is actually “disclosed” through use of electric utilities are likely to change.

This is illustrative of the primary issue in Naperville Smart Meter Awareness: smart meters are the next major iteration of intrusive home technology, and public opinion is likely to change as the technology grows more sophisticated. Further, smart meters are not limited to electric utilities; gas companies have also begun implementing use of the technology. Thus, it is unsound for the judiciary to set precedent in an area that is volatile and subject to change. Moreover, the Seventh Circuit’s treatment of the “reasonable” issue – revolving around

---

170 Id.
171 Id. at 418.
172 Id.
173 Id. at 429–30.
174 Id.
175 See supra notes 140-141.
infrastructural priorities and costs – should not undermine what constitutes a “reasonable” search.

This calls into question how Fourth Amendment privacies can be reconciled with municipal needs. The City of Naperville’s citizens were given no voice in the smart meter upgrade, nor could they take their electrical needs to another company because the municipality is the sole electric provider. Thus, there are competing interests between citizen privacy and government interests. There are two plausible ways to reconcile the two with the Fourth Amendment: (1) citizens would presumably need to voluntarily consent to smart meter installation (and therefore freely share their usage data); or (2) a court would have to find that there is no reasonable expectation of privacy in the data. Yet, it would be almost impossible for a court to fulfill that second task, provided that the data would not exist but for the technology itself. Moreover, the data reveals intimate details within a home that, absent the smart meters, would not be available to utility providers or, potentially, local law enforcement. The smart meter data reveals “intimate details of the home” within the meaning of Fourth Amendment precedent, and without voluntary consent, it is difficult to see how citizens would not have a reasonable expectation of privacy in those intimate details.\textsuperscript{176}

A bright line rule of what is “reasonable,” or any attempts at a sliding scale approach that weighs parties’ interests against one another, are ill-conceived, impractical, and lack a foundation in Fourth Amendment jurisprudence. In his Carpenter dissent, Justice Kennedy noted that the Court found that officials crossed “a constitutional line” by obtaining more than six days of cell-site records.\textsuperscript{177} He characterized this finding as “illogical” and something that will “frustrate principled application of the Fourth Amendment” in “vital law enforcement operations.”\textsuperscript{178} While Justice Kennedy’s concerns may not yet be true of smart meter data, court application of the Fourth

\textsuperscript{178} Id.
Amendment is intended to anticipate major technological change.\textsuperscript{179} As such, setting untenable precedent now regarding how and when a Fourth Amendment search is reasonable, and the factors applicable to the same, is ill advised. The Seventh Circuit’s holding generally permits utility providers, including the City of Naperville, to amass intimate details regarding its customers’ homes and to store the data for up to three years without customer consent.\textsuperscript{180} Courts almost universally consider the “slippery slope” argument, refusing to set precedent where it could harm future plaintiffs through generalizations and expansions of precedential principles. The Seventh Circuit’s analysis and holding in \textit{Naperville Smart Meter Awareness} is threatening for this reason.

Even more troubling is what the Seventh Circuit does not discuss: the implications for permitting this amassing of data. Though there are no criminal charges at issue in \textit{Naperville Smart Meter Awareness}, like those in \textit{Carpenter}, the implications for the use of this data in a criminal investigation remain operative. After all, what is to stop law enforcement from, after years of data collection, accessing this data as part of an ongoing investigation? Without the smart meter data, there would be no data detailing intimate usage patterns within a home. And, because the data can hypothetically be stored for years, the precedent here will intrusively alter law enforcement’s access to information that may lead to convictions whereas before, that information did not exist. The City of Naperville’s citizens were not given a choice in whether they had a smart meter installed. As such, the forced installation of the smart meters, which store information that could, at an undeterminable future date, be used as part of an investigation is the real question the court should consider in \textit{Naperville Smart Meter Awareness}. The Seventh Circuit even cautioned that the holding could be different depending on the accessibility of the data at issue to law enforcement.\textsuperscript{181}

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{179} \textit{Id.} (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928)).
\item \textsuperscript{180} \textit{Naperville Smart Meter Awareness v. City of Naperville}, 900 F.3d 521, 524 (7th Cir. 2018).
\item \textsuperscript{181} \textit{Id.} at 529.
\end{enumerate}
\end{footnotesize}
crystal ball, there is no way of knowing how the information may be used at a future date. However, it is clear that today, the Seventh Circuit’s holding plainly violates Fourth Amendment rights and uses a factor-based interest analysis to hold that government interests outweigh fundamental liberties granted in the Bill of Rights.

C. Proposed Change/Analysis

Fourth Amendment rights weigh in favor of the citizens and shield them from law enforcement and other parties with “arbitrary power” that might wrongfully obtain access to certain records. The Seventh Circuit justified the City of Naperville’s collection of electric usage in fifteen-minute intervals because smart meters provide for more efficient power restoration, reduce strain on the power grid, and reduce labor costs. Weighing these interests against one another, and qualifying the holding with notes as to how minor differences in fact – such as the interval of data collection – may affect the holding is akin to the distinction Justice Kennedy set forth in Carpenter. After all, smart meter technology is still in its early stages. Thus, like the thermal imaging technology at issue in Kyllo, which, though rudimentary at the time, still constituted an unreasonable search, the more advanced data available via smart meters should follow the same logic. After all, the underlying Act – the American Recovery and Reinvestment Act of 2009 (“Recovery Act”) – is not yet a decade old. Thus, the Seventh Circuit is setting precedent in an area where the technology is arguably not yet in “general public use.”

---

183 Naperville Smart Meter Awareness, 900 F.3d at 528–29.
184 Carpenter, 138 S. Ct. at 2234 (Kennedy, J., dissenting).
187 Kyllo, 533 U.S. at 27.
The primary issue with the Seventh Circuit’s holding in *Naperville Smart Meter Awareness* is the court’s attempt to draw the same, fine line of what is “reasonable,” as the *Carpenter* Court did. By way of example, the Seventh Circuit held, based off of subjective factors, that fifteen-minute interval utility data collection was reasonable when weighed against substantial government interests.\(^{188}\) The court focused on the City of Naperville’s interests, along with the Federal Government’s interests, in updating the power grid based on the 2009 Recovery Act.\(^{189}\) Yet, the court provided other justifications for its holding relating to consumers, who were given no legitimate choice whether their traditional meters were upgraded.\(^{190}\) For example, the court emphasized that smart meters allow quicker utility restoration after an outage and time-based pricing.\(^{191}\) The court further provided that the City of Naperville could have avoided the controversy altogether “by giving its residents genuine opportunity to consent to the installation of smart meters, as many other utilities have.”\(^{192}\)

This analysis, coupled the phrasing of the *Naperville Smart Meter Awareness* test, is a weaker version of the strict scrutiny standard that must be used when a fundamental right is at issue.\(^{193}\) The Fourth Amendment, as part of the Bill of Rights, confers fundamental rights to citizens of the many states through the Fourteenth Amendment.\(^{194}\) Thus, strict scrutiny should be applied.\(^{195}\) This means that there must be a compelling state interest, the legal provision must be narrowly tailored to accomplish that interest, and the legal provision must

\(^{188}\) *Naperville Smart Meter Awareness* v. City of Naperville, 900 F.3d 521, 528–29 (7th Cir. 2018).
\(^{189}\) *Id.* at 524.
\(^{190}\) *Id.*
\(^{191}\) *Id.* at 528.
\(^{192}\) *Id.* at 529.
\(^{193}\) In *re R.C.*, 195 Ill. 2d 291, 303 (Ill. 2001).
\(^{194}\) U.S. CONST. amend. XIV.
\(^{195}\) In *re R.C.*, 195 Ill. 2d at 303.
accomplish that interest by the least restrictive means available.\textsuperscript{196} The Seventh Circuit reasoned along different parameters, finding that the “search,” here the collection of smart meter data, must be “reasonable.”\textsuperscript{197} Yet, nowhere in the opinion does the Seventh Circuit mention that the City of Naperville and Federal Government had a “compelling” interest in installation of the meters. Instead, the Seventh Circuit weighed citizen privacy interests with the government’s interest in data collection,\textsuperscript{198} holding that the benefits stack in the favor of the government’s interest and, that because “the search is unrelated to law enforcement, is minimally invasive, and presents little risk of corollary criminal consequences,” it was reasonable.\textsuperscript{199} This less rigorous standard supports the Seventh Circuit’s holding while obliterating fundamental rights. An interest analysis in any Fourth Amendment context does not appreciate the scope and importance of what is at stake, something markedly absent from the Seventh Circuit’s opinion and consideration of this matter.

Thus, the crux of the court’s holding is based on consumer-focused factors, all while Naperville Smart Meter Awareness’ primary complaint is that there cannot be a voluntary disclosure of this information to the utility provider because citizens were given no meaningful choice in the installation of the smart meters.\textsuperscript{200} It is counterintuitive for a court to model a holding on consumer-focused interests when consumers are the individuals objecting to this data collection. This undermines Fourth Amendment protections and precariously overlooks what will become increasingly sensitive data as smart meter technology advances, shorter intervals are recorded, or the data is used by law enforcement with increasing regularity. Because Naperville Smart Meter Awareness focused solely on the collection of this data in the ordinary course of business, any criminal implications

\textsuperscript{196} In re D.W., 214 Ill. 2d 289 (2005); Schultz v. Lakewood Elec. Corp., 362 Ill. App. 3d 716 (1st Dist. 2005), appeal denied, 218 Ill. 2d 557 (Mar. 29, 2006).

\textsuperscript{197} Naperville Smart Meter, 900 F.3d at 527–29.

\textsuperscript{198} Id.

\textsuperscript{199} Id. at 529.

\textsuperscript{200} Id. at 527.
likely to arise in these other situations are not yet at issue. However, inaction unless and until a case arises where smart meter data is used in a criminal matter is nonsensical. Constitutional rights were violated, and these rights should be addressed before smart meters proliferate and utility companies begin amassing this data. This further emphasizes the dangers of the Seventh Circuit opinion, as the court was not overly protective of intimate details – data from within the home and not readily available without smart meter technology.\footnote{See United States v. Karo, 468 U.S. 705, 735 (1984) (finding that a “search” began when Karo brought the can of ether into his home as it was “concealed from view”); Arizona v. Hicks, 480 U.S. 321 (1987) (finding a search where the officers searched for the serial number on stereo equipment in “plain view” in the alleged suspect’s home).}

Mr. Wessler’s suggestion that certain types of searches are “reasonable” or “unreasonable” without a warrant is similarly tenuous.\footnote{Transcript of Oral Argument at 33–34, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).} In fact, his suggestion that thermostat data is inclusive of what can be properly categorized\footnote{Id.} as either reasonable or unreasonable stands in contradiction to longstanding case law.\footnote{See, e.g., Kyllo v. United States, 533 U.S. 27 (2001).} Any data pertaining to the interior of a home that would be unavailable without the use of some technology to collect said data constitutes a search.\footnote{Id.} To find that any category of data is reasonable without a warrant ignores the particular facts and circumstances of any case that comes before the court. This is something the Seventh Circuit emphasized as critical in its \textit{Naperville Smart Meter Awareness} analysis.\footnote{Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 529 (7th Cir. 2018).} For example, had the intervals been shorter, the Seventh Circuit’s holding in \textit{Naperville Smart Meter Awareness} might have been different.\footnote{Id.} Enacting specific categories is problematic for these
reasons, and courts should exercise extreme caution when considering similar issues on a case-by-case basis.

IV. CONCLUSION

The Seventh Circuit is the first federal court to render a decision regarding smart meter data in the context of the Fourth Amendment. As this technology continues to proliferate and improve in accordance with the Recovery Act, more courts will likely rule on the same issue. *Naperville Smart Meter Awareness* presented a contentious question to the Seventh Circuit because citizens lacked any meaningful choice of whether intimate details within the home were disclosed to the City of Naperville as the sole electric utility provider. Generally speaking, the precarious weighing of various subjective factors and interests was, and will continue to be, unconstitutionally under-protective and problematic, as would be the enumeration of discrete categories of data that should or should not be protected.

The Fourth Amendment’s language does not change in the same manner that technology does, but a court’s interpretation of its basic protections, as applied to that technology, must. It is important that Fourth Amendment rights are granted the same protection in all contexts as technology proliferates, advances, and grows more intrusive in the home. All courts should proceed on a case-by-case basis in weighing smart meter data and whether a search of that data is reasonable. Where there are violations of the fundamental rights safeguarded by the Fourth Amendment, it is essential that courts use a strict scrutiny standard before eliminating those rights.

There will never be neat categories of technology that should or should not constitute a “reasonable search.” Whether a search is reasonable will be context-specific and depend on several factors, such as the length of the data collection or whether an individual knowingly revealed the data to a third party or otherwise. However, it should never be dependent on what it reveals, as a search of the home is a search of the home regardless of what data that search produces. Any lingering uncertainties must be addressed under strict scrutiny.
analysis, which will almost certainly occur in the near future as smart meters continue to spread across the United States.