UNC SCHOOL OF LAW

NORTH CAROLINA LAW REVIEW

Volume 99 | Number 4 Article 7

5-1-2021

The Fourth Amendment in Your Shower: Naperville, Reasonable Expectations of Privacy, and the Intimate Nature of Electric Smart Meter Data

Alexandra Franklin

The Fourth Amendment in Your Shower: *Naperville*, Reasonable Expectations of Privacy, and the Intimate Nature of Electric Smart Meter Data*

Electric smart meters are touted by energy experts as incredibly helpful tools for increasing the responsiveness and efficiency of the electricity grid by predicting consumer usage in a real time manner. However, real time responses require real time reporting, meaning that smart meters are documenting the movements and activities of every consumer connected to them. Whether someone prefers to take a shower at night, whether they were home on a particular day, or even what movie they were watching a year ago—this information is readily accessible to any trained eye with access to a consumer's smart meter data, and law enforcement agencies are taking notice of its potentially limitless benefits in criminal cases.

As smart meters become more ubiquitous, Fourth Amendment concerns are heightened. In 2018, the Seventh Circuit addressed this burgeoning sphere of privacy concerns in Naperville Smart Meter Awareness v. City of Naperville. *The court acknowledged that smart meter data collection by a government-run utility constitutes a search—but a reasonable one, nevertheless.*

This Recent Development argues that the Seventh Circuit both downplayed the invasiveness of electric smart meter data and its potential criminal implications and overlooked significant Supreme Court precedent by failing to address the fact that smart meter data encroaches on the most protected sphere in Fourth Amendment jurisprudence—the home. Additionally, the Seventh Circuit's other fundamental flaw was dismissing an element of smart meter data collection that makes it particularly dangerous—its ability to collect hundreds of thousands of data points over time, providing those who access the data a wealth of information otherwise unknowable via any other traditional search tool.

This Recent Development asserts that these oversights were critical. The nature of smart meter data collection embodies some of the most fundamental concerns in Fourth Amendment privacy jurisprudence. The sheer invasiveness of unfettered data access warrants a bright-line rule against individualized, granular data collection by government agencies—including government-owned utilities—absent a warrant or consent. Importantly, this solution poses minimal

burdens on government-run utilities, as there are various tools available to protect consumer privacy without compromising grid resiliency.

INTRODUCTION

In the last 250 years, what began as Benjamin Franklin's single filament light bulb has evolved into a complex, electrical grid. This grid, powered by massive power plants, is able to respond to demand almost instantaneously. Electricity is an essential resource in nearly every facet of life, from global manufacturing and production industries to the most intimate and personal activities we engage in. Life in the twenty-first century necessitates interconnectedness with the electrical grid in every aspect of our lives. However, as electricity infiltrates every crevice of American society, the demands of a modern grid system, privacy principles, and the Fourth Amendment are on a collision course, and courts have deferred their obligation to prevent this train wreck.

In *Naperville Smart Meter Awareness v. City of Naperville*,[1] the Seventh Circuit addressed an emerging area of data privacy concern—electric smart meters. Particularly, it considered whether a city-owned utility's use of these meters constituted an unreasonable search under the Fourth Amendment.[2] The court determined that the data collection did constitute a search—but a reasonable one. When balancing the "intrusion on the individual's Fourth Amendment interests against its promotion of legitimate government interests,"[3] the court found that the value of the data collection in ensuring a reliable electricity grid outweighed a customer's privacy interests.[4] Critically, the court determined that the data was collected with "no prosecutorial intent."[5] According to the Seventh Circuit, the data collection lacked criminal implications, so the privacy interests were less significant than privacy interests in prior Fourth Amendment cases.[6]

However, this conclusion of reasonableness failed to account for central elements of smart meter data usage that pose a greater risk than the court implied—namely where the search occurs and how often it is conducted. This Recent Development explores how the *Naperville* court downplayed the gravity of an individual's privacy interests in establishing the reasonableness of the search. It then advocates for a bright-line rule that prohibits governmental access to granular, individually identifiable data absent a warrant or consent. A judicial view of electricity data that fully contemplates the potential dangers of

1. 900 F.3d 521 (7th Cir. 2018).
2. *Id.* at 525.
3. *Id.* at 528 (quoting Hiibel v. Sixth Jud. Dist. Ct., 542 U.S. 177, 187–88 (2004)).
4. *Id.* at 529.
5. *Id.* at 528.
6. *Id.*

unbridled governmental access—irrespective of prosecutorial intent—can simultaneously respect the growing governmental need for such data, while also shielding individuals from surveillance-state fears.

Analysis proceeds in five parts. Part I explores the intersection of Fourth Amendment analysis and privacy law amid the proliferation of digitized information. Part II provides background on the advent of electric smart meters and their role in the modern electricity system, as well as the *Naperville* decision and its reasonableness conclusion. Part III explains why *Naperville*'s "prosecutorial intent" inquiry minimized the constitutional concerns associated with the search. Part IV identifies two main areas in which *Naperville* fell short in its analysis—failing to consider the significance of searches within the home and downplaying the heightened privacy implications involved in longitudinal searches. Part V proposes a bright-line judicial rule for governmental data collection within the home.

I. THE EVOLUTION OF FOURTH AMENDMENT SEARCHES AND PRIVACY CONCERNS

The Fourth Amendment protects individuals against unreasonable searches by the government.[7] However, as society has evolved, so has the Supreme Court's understanding of what constitutes a search. The Fourth Amendment was originally based on a common-law trespass theory, meaning that a search had to involve a physical invasion on a constitutionally protected space.[8] However, Justice Harlan's concurrence in *Katz v. United States*[9] facilitated an additional lens through which courts began viewing searches[10]—whether a search violates a person's "reasonable expectation of privacy."[11] This additional analytical aspect recognizes that "the Fourth Amendment protects people, not places"[12] and that technological innovation allows the government to intrude on "areas normally guarded from inquisitive eyes."[13] This test has become commonplace when courts evaluate whether the government's actions constituted a search.[14] It asks (1) whether the individual had a reasonable

7. U.S. CONST. amend. IV.

8. *See* United States v. Jones, 565 U.S. 400, 404–05 (2012).

9. 389 U.S. 347 (1967).

10. *See Jones*, 565 U.S. at 409 ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

11. *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

12. *Id.* at 351 (majority opinion).

13. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

14. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34–35 (2001) (referencing the common-law tradition of respecting the interior of homes as private to conclude that thermal imaging directed at the defendant's home violated the defendant's expectation of privacy); Florida v. Riley, 488 U.S. 445, 450 (1989) (finding the defendant did not have a reasonable expectation of privacy in a greenhouse visible

expectation of privacy and (2) if society is willing to recognize that expectation.[15] The reasonable expectation of privacy test has been used to evaluate whether the use of numerous technological devices constitute a search under the Fourth Amendment, including GPS monitoring,[16] thermal-imaging tools,[17] and cell-site data.[18]

In 2010, the D.C. Circuit in *United States v. Maynard*[19] introduced the idea that privacy concerns are heightened when a search is conducted on a continuous, rather than discrete, basis.[20] In *Maynard*, police placed a tracking device on the defendant's car for twenty-eight days, continuously collecting information on his whereabouts without a warrant.[21] In evaluating the strength of the defendant's privacy interests, the court held that the continuous nature of the data collection was distinct because it equated to an aggregation of searches rather than an individualized search.[22] The D.C. Circuit then noted that a reasonable person "expects each of those movements to remain 'disconnected and anonymous.'"[23]

The Supreme Court later affirmed *Maynard* in *United States v. Jones*,[24] but under the traditional physical trespass theory of a search.[25] However, separate concurrences by Justices Alito and Sotomayor collectively garnered the support

from an aircraft); California v. Ciraolo, 476 U.S. 207, 211 (1986) (using the reasonable expectation of privacy test to determine that a warrantless aerial search of the defendant's fenced backyard was unreasonable); Rakas v. Illinois, 439 U.S. 128, 148 (1978) (holding that passengers in a getaway car did not have a reasonable expectation of privacy in their belongings located inside the car since they had "neither a property nor a possessory interest" in the vehicle).

15. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

16. *See* United States v. Jones, 565 U.S. 400, 402 (2012).

17. *Kyllo*, 533 U.S. at 34–35; *see also* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 526 (7th Cir. 2018) ("What's more, the data collected by Naperville can be used to draw the exact inference that troubled the Court in *Kyllo*. . . . In fact, the data collected by Naperville could prove even more intrusive.").

18. *Carpenter*, 138 S. Ct. at 2213–14.

19. 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom*. United States v. Jones, 565 U.S. 400 (2012).

20. *Id.* at 558 ("[T]he whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts.").

21. *Id.*

22. *Id.* at 563–64 ("Society recognizes Jones's expectation of privacy in his movements over the course of a month as reasonable, and the use of the GPS device to monitor those movements defeated that reasonable expectation.").

23. *Id.* at 563 (quoting Nader v. Gen. Motors Corp. 255 N.E.2d 765, 772 (N.Y. 1970) (Breitel, J., concurring)).

24. 565 U.S. 400 (2012).

25. *Id.* at 404–05. The majority opinion, authored by Justice Scalia, held that the installation of a continuous GPS monitoring device on Jones's vehicle violated the Fourth Amendment because installation of the device constituted a physical trespass—focusing on the "installation" of the device itself rather than the substance of the data it collected. *Id.* at 402, 404–05.

of a majority of the Supreme Court Justices.[26] These concurrences upheld the root of the *Maynard* decision—that the data collection in the aggregate was a Fourth Amendment violation because the continuous collection of information violated the reasonable expectation of privacy test.[27]

The *Maynard* decision and *Jones* concurrences gave credence to the "Mosaic Theory," which posits that "individual pieces of otherwise unimportant information, when grouped together, can amount to important intelligence information that requires high-level confidential treatment."[28] Since *Maynard* and *Jones*, courts have grappled with how to operationalize the Mosaic Theory. The *Jones* concurrences acknowledge that their conclusions fail to create a precise formula as to when technological surveillance crosses the threshold of unreasonableness, but these cases present "an encouraging step toward a more contextual approach to digital privacy."[29] In particular, the *Katz*-to-*Jones* evolution indicates that social norms are critical to evaluating the strength of an individual's privacy interest by focusing on places in which society is unwilling to accept government searches.

With this background established, the following part explores a new technology to which Fourth Amendment principles are being applied—electric smart meters. It then addresses the Seventh Circuit's dismissal of privacy concerns regarding the government's unfettered access to smart meter data.

II. ELECTRIC SMART METERS AND *NAPERVILLE*'S REASONABLENESS CONCLUSIONS

The critical point of contention in *Naperville* involved a municipally owned electric utility's modernization efforts.[30] Using a federal grant aimed at

26. *See id.* at 413 (Sotomayor, J., concurring); *id.* at 418 (Alito, J., concurring). Justice Alito's concurrence—which garnered the support of Justices Ginsburg, Breyer, and Kagan—focused exclusively on how the defendant's reasonable expectation of privacy "were violated by the long-term monitoring of the movements of the vehicle [the defendant] drove" and argued that the majority's focus on the physical trespass was "highly artificial." *Id.* at 419 (Alito, J., concurring). Justice Sotomayor's concurrence supported the majority's use of the physical trespass test but also noted that the use of the long-term GPS monitoring device violated Jones's expectation of privacy. *Id.* at 414–15 (Sotomayor, J., concurring).

27. *Id.* at 415 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

28. Jessica Gutierrez-Alm, *The Privacies of Life: Automatic License Plate Recognition Is Unconstitutional Under the Mosaic Theory of Fourth Amendment Privacy Law*, 38 HAMLINE L. REV. 127, 142–43 (2015).

29. Natasha H. Duarte, *The Home out of Context: The Post-*Riley *Fourth Amendment and Law Enforcement Collection of Smart Meter Data*, 93 N.C. L. REV. 1140, 1143 (2015).

30. It is important to note that the governance of the utility is critically important for purposes of this Recent Development. Since the Fourth Amendment protects individuals from unreasonable searches conducted by the *government*, had the residents of Naperville received their electricity from a

improving electricity grid resilience, Naperville's government-owned utility installed electric smart meters into all residential homes.[31] Although the case centered around one city's use of smart meters, the City of Naperville is part of a more widespread movement to incorporate these devices into the electricity grid. This part contextualizes the case by first exploring the functionality of smart meters and their relevance to efficiency and modernization efforts in the electric power sector. It then examines the arguments presented in *Naperville*.

A. *Electric Smart Meters and the Smart Grid Transition*

Electric smart meters are distinct from traditional analog meters because they facilitate a digital two-way communication between a customer's home and the utility.[32] This allows the utility to remotely collect electricity-consumption data from an individual's home at regular intervals throughout the day, whereas analog meters only furnish data on the total energy consumption for the prior billing period and require a utility employee to physically travel to each customer's home to record consumption information for monthly bill purposes.[33] Smart meters are seen as a critical tool in transitioning into a modern "smart grid" because the near real time data generated by the meters poses several efficiency benefits.[34] Primarily, customers' granular energy consumption data can be made available to them, permitting those consumers to adjust their daily use habits in order to create personal cost savings, while also increasing the energy efficiency of the utility grid at large.[35] This is particularly relevant during peak usage times when a utility would traditionally turn on "peaker" plants—energy plants reserved exclusively for high-demand times.[36] These plants are incredibly expensive to run and often spew greenhouse gases into low-income communities, raising both cost efficiency and

privately owned electric utility, then the application of the Fourth Amendment would be distinctly different. In that instance, the connection to government access would be more attenuated, and other Fourth Amendment principles such as the third-party doctrine would apply. *See* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018) ("Before continuing, we address one wrinkle to the search analysis. Naperville argues that the third-party doctrine renders the Fourth Amendment's protections irrelevant here. . . . This argument is unpersuasive. . . . There is no third party involved in the exchange."). For an application of the Fourth Amendment to smart meter data owned by private utilities, see generally Sarah Murphy, Note, *Watt Now? Smart Meter Data Post-*Carpenter, 61 B.C. L. REV. 785 (2020).

31. *Naperville*, 900 F.3d at 524.

32. *See* Hayden McGovern, *What Is a Smart Meter?*, SMART ENERGY (Dec. 16, 2016), https://www.smartenergy.com/what-is-a-smart-meter/ [http://perma.cc/5SCY-K8KW].

33. *See id.*; *see also* U.S. DEP'T. OF ENERGY, SMART GRID SYSTEM REPORT: 2018 REPORT TO CONGRESS 13 (2018) [hereinafter SMART GRID SYSTEM REPORT].

34. *See* SMART GRID SYSTEM REPORT, *supra* note 33, at 11.

35. *The Benefits of Smart Meters*, CAL. PUB. UTILS. COMM'N, https://www.cpuc.ca.gov/general.aspx?id=4853 [https://perma.cc/M7AE-JALT].

36. *See id.*

environmental justice concerns.[37] However, because smart meters provide a utility with constant data on consumer use, the utility can leverage efficiency programs such as time-of-use rates to incentivize consumers to lower their personal electricity use during peak times, reducing the need for the high-cost plants.[38]

Further, the data generated by smart meters contains far more information than just a general description of a consumer's overall electricity use. All appliances and other electricity-dependent products in our homes contain specific load signatures, meaning these objects use electricity in such distinct ways that the electric utility can identify specifically what type of activity is occurring within a household at any given time.[39] Thus, a trained eye could evaluate which households on a city block prefer taking showers in the morning, which eat microwave meals for every dinner, or what day of the week a family washes all their laundry.[40] This kind of continuous, granular data collection allows a utility to adjust its power output in a significantly more efficient manner than a traditional analog meter, converting the retrospective process of examining energy use, monitoring outages, and adjusting power sources into a substantially more responsive process.[41] Because smart meters provide numerous benefits for utilities, their use has exploded in the United States in the last decade. In fact, by 2030, ninety-three percent of all U.S. customers are expected to be connected to their electricity provider with a smart meter.[42]

B. Naperville *and Fourth Amendment Concerns*

Given the significant advantages from both an administrative and energy efficiency perspective, it is of little surprise that the City of Naperville was a willing participant in smart meter adoption. However, although smart meters

37. *See* PEAK COAL., DIRTY ENERGY, BIG MONEY: HOW PRIVATE COMPANIES MAKE BILLIONS FROM POLLUTING FOSSIL FUEL PEAKER PLANTS IN NEW YORK CITY'S ENVIRONMENTAL JUSTICE COMMUNITIES—AND HOW TO CREATE A CLEANER, MORE JUST ALTERNATIVE 5 (2020), https://www.cleanegroup.org/wp-content/uploads/Dirty-Energy-Big-Money.pdf [https://perma.cc/VT7Q-NJZY] ("Over the last decade, an estimated $4.5 billion of ratepayer money—in the form of what are called 'capacity payments'—have gone to the owners of the city's peaker plants, simply to keep peakers online in case they may be needed."); PSE HEALTHY ENERGY, CALIFORNIA PEAKER POWER PLANTS: ENERGY STORAGE REPLACEMENT OPPORTUNITIES 1 (2020), https://www.psehealthyenergy.org/wp-content/uploads/2020/05/California.pdf [https://perma.cc/6WRH-E89X] ("Half of [California's peaker plants] are located in areas designated as *disadvantaged communities* by the state of California due to high cumulative socioeconomic, environmental, and health burdens.").

38. *See The Benefits of Smart Meters*, *supra* note 35.

39. *See* CONG. RSCH. SERV., R42338, SMART METER DATA: PRIVACY AND CYBERSECURITY 3–5 (2012), https://fas.org/sgp/crs/misc/R42338.pdf [https://perma.cc/2KHT-6WE7].

40. For a striking visual depiction of how load signatures reveal a household's specific activities, see *id.* at 5 fig.I.

41. *See* SMART GRID SYSTEM REPORT, *supra* note 33, at 27.

42. *Id.* at 30 fig.10.

are largely praised as necessary tools in shifting to a cleaner and more efficient electricity grid, *Naperville* highlights the imminent concerns that emerge when these data-mining tools are operated by a government-owned electric utility.

The digital meters installed in *Naperville* allowed the municipal utility to remotely capture energy consumption data from residents at fifteen-minute intervals and store this data for three years.[43] The 148,000 residents of Naperville[44] were not allowed to opt out of smart meters[45] but were instead provided with a Smart Grid Bill of Rights that ensured the data would not be distributed to third parties absent a warrant.[46] In 2015, Naperville Smart Meter Awareness ("NPSA"), a nonprofit organization formed by the residents of Naperville, brought suit against the utility alleging Fourth Amendment violations emerging from the utility's unfettered access to such personal data.[47] The federal district court dismissed the claims, and NPSA appealed.[48]

The Seventh Circuit began its analysis by establishing that the use of smart meter data constituted a search under the Fourth Amendment.[49] While not a physical search in the traditional sense, the nature of the data collection facilitated the government's ability to "explore details of the home that would previously have been unknowable without physical intrusion."[50] The court then proceeded to evaluate the reasonableness of the search by balancing the intrusion on individuals' Fourth Amendment rights against the promotion of legitimate government interests.[51]

43. Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 524 (7th Cir. 2018). Utilities can choose the intervals at which they collect data and store it. Other utilities may, and do, use more frequent time intervals to transmit the consumption data from the meter. *See* McGovern, *supra* note 32.

44. *About Naperville*, CITY NAPERVILLE, https://www.naperville.il.us/about-naperville/ [https://perma.cc/5G29-X2R9].

45. *Naperville*, 900 F.3d at 524. The City of Naperville utility generally collects electricity-consumption data via radio frequency communication. Individuals are permitted to opt out of automated data collection but still must pay both an installation and monthly fee for the service. Nonetheless, even when opting out of the radio frequencies, the smart meters still capture data at the same fifteen-minute intervals and provide the utility with the same information when the data is physically retrieved. Naperville Smart Meter Awareness v. City of Naperville, 114 F. Supp. 3d 606, 609 (N.D. Ill. 2015), *aff'd*, 900 F.3d 521 (7th Cir. 2018).

46. *Naperville*, 900 F.3d at 528; NAPERVILLE, ILL., CODE OF ORDINANCES § 8-0.5-2(2)(E) (LEXIS through Ordinance No. 21-007). Notably, the Smart Grid Bill of Rights begins by asserting that data will categorically not be released to third parties, but in a later bullet point clarifies that third-party access would be granted via a warrant, court order, or customer consent. *Id.* For a discussion as to why the Smart Grid Bill of Rights does not damper Fourth Amendment concerns, see *infra* Section III.A.2.

47. *Naperville*, 114 F. Supp. 3d. at 608–09.

48. *Id.* at 612–13.

49. *Naperville*, 900 F.3d at 527.

50. *Id.* at 526 (quoting Kyllo v. United States, 533 U.S. 27, 40 (2001)).

51. *Id.* at 528.

Because smart meter installation was not inherently related to prosecutorial actions, the court's analysis of individual privacy interests was based solely on a comparison between Naperville's data collection and jurisprudence on administrative searches within the Fourth Amendment context.[52] The Seventh Circuit drew a distinction between the data collection in Naperville and an administrative search for building code compliance. Because the data collection did not require physical entry into an individual's home, as was the case with administrative searches, the court characterized it as "minimally invasive."[53] Moreover, unlike administrative searches where the fruits of the search could immediately result in a criminal citation, smart meter usage lacked an immediate risk of corollary criminal implications, which in the eyes of the court, attenuated the connection between privacy expectations and electricity usage.[54] And finally, when the seemingly innocent data collection was viewed in combination with the city's Smart Grid Bill of Rights, consumer privacy interests were "more limited."[55]

Despite accounting for the potential dangers of the data collection within its determination that smart meter usage constituted a search, the court did not extend this analysis in evaluating the strength of an individual's privacy interest while determining the reasonableness of the search. Instead, after noting the distinctions between the data collection and administrative searches, the court acknowledged the government's substantial interest in collecting the information.[56] Thus, the "minimally invasive" search in comparison to national grid modernization goals heavily tipped the scales in favor of the City of Naperville, overcoming the presumption of unreasonableness.[57]

III. *NAPERVILLE*'S "PROSECUTORIAL INTENT" INQUIRY SHORT-CIRCUITED PROPER ANALYSIS OF THE NATURE OF THE SEARCH

The Seventh Circuit's conclusion of reasonableness was based on an incomplete assessment of the nature of electric smart meter data collection and failed to account for critical similarities between the *Naperville* search and modern Fourth Amendment precedent. This sparse inquiry overlooked critical privacy interests implicated in the search. The following sections first explore how *Naperville's* exclusive focus on prosecutorial intent mischaracterized the role smart meter data plays in modern criminal cases and then identifies the

52. *Id.*; United States v. Bulacan, 156 F.3d 963, 967 (9th Cir. 1998) (stating that administrative searches are those that are "conducted as part of a general regulatory scheme, done in furtherance of administrative goals rather than to secure evidence of a crime").

53. *Naperville*, 900 F.3d at 529.

54. *Id.* at 528–29.

55. *Id.* at 528.

56. *Id.*

57. *Id.* at 529.

gaping holes in the court's analysis by pinpointing critical Fourth Amendment considerations the court overlooked.

A. *Sitting in the Dark:* Naperville*'s Deficient Comparison to Administrative Searches*

While *Naperville* was unique from traditional Fourth Amendment search cases because the search was conducted outside of a criminal context, the noncriminal nature of a search does not lessen an individual's interest in ensuring intimate details of their life are free from governmental intrusion.[58] However, the fact that the search was conducted without prosecutorial intent was the crux upon which the *Naperville* court fastened its conclusion that the government's interest in the data was greater than an individual's interest in retaining their confidentiality—and served as the court's only analysis into individual privacy interests.[59]

1. *Camara* Prescribes a More Thorough Evaluation of Privacy Interests

The *Naperville* court relied on *Camara v. Municipal Court of San Francisco*[60] for its assertion that a lack of prosecutorial intent justified a reduction in an individual's privacy interest.[61] In *Camara*, an individual living in an apartment refused to allow a building code inspector to enter his home without a warrant, resulting in the city issuing him a criminal citation.[62] The Supreme Court found that warrantless administrative searches were unconstitutional under the Fourth Amendment because an individual's privacy interests in the sanctity of their home exceeded even a government's desire to prevent devastating "fires and epidemics."[63] Instead, the probable cause standard and the "warrant machinery" would ensure inspections protected individuals' privacy expectations.[64]

The Seventh Circuit distinguished the search in *Naperville* from the search in *Camara* by contrasting the likelihood of criminal prosecution between building code inspections and smart meter usage. *Camara*, however, prescribed a more thorough method of incorporating this factor into Fourth Amendment reasonableness conclusions. In its opinion, the *Camara* Court did assert that a

58. *See* David Alan Sklansky, *Too Much Information: How Not To Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1120 (2014) ("[I]t is difficult to imagine any delineation of the private sphere that does not include a space for intimacy: not just for physical intimacy, but for expressing thoughts and feelings to oneself and to one's intimate acquaintances without sharing them with the world. Some forms of electronic monitoring seem inconsistent with respect for any such space."); *supra* text accompanying notes 49–52; *infra* text accompanying notes 61–63.

59. *Naperville*, 900 F.3d at 528.

60. 387 U.S. 523 (1967).

61. *Naperville*, 900 F.3d at 528.

62. *Camara*, 387 U.S. at 525.

63. *Id.* at 535.

64. *Id.* at 532–33.

search conducted without prosecutorial intent renders it a "less hostile intrusion."[65] However, the Court also stated that the ability of the government to leverage platonic administrative searches for future prosecution was significant and that "it is surely anomalous to say that the individual and his private property are fully protected by the Fourth Amendment only when the individual is suspected of criminal behavior."[66] Accordingly, the discussion in *Camara* regarding the lack of prosecutorial intent was merely the beginning of its analysis of privacy interests. The Supreme Court still proceeded in a lengthy assessment of individual interests in retaining privacy within their homes, even from building code inspectors seeking to prevent significant community harm.[67]

In *Camara*, the Court addressed the government's assertion that warrants were unnecessary for building code inspections because the search was crafted to "make the least possible demand" on occupants,[68] the ordinances authorizing these inspections were "hedged with safeguards,"[69] and the policy reasoning behind the inspections made them ill-suited for review by a magistrate in order to obtain a warrant.[70] All of these justifications for bypassing a warrant requirement fell short because they "unduly discount[ed] the purposes behind the warrant machinery."[71] Instead, a warrantless system would render occupants subject to the total discretion of the inspector, and "[t]his is precisely the discretion to invade private property which [the Court] ha[s] consistently circumscribed."[72] A warrant issued by a neutral, detached magistrate would ensure that the searches were sufficiently tailored to serve the inspection's purpose and actually necessary—not subject to the whims of an interested party.

In stark contrast to the *Camara* Court, the *Naperville* court used the platonic nature of the search as a method of discrediting an individual's privacy interest, without ever exploring what privacy interests were actually implicated.[73] In reality, the Court's decision in *Camara* bolsters the idea that a prosecutorial-intent inquiry is properly addressed separately from an evaluation of the relative significance of both an individual's and the government's interests. In this way, the prosecutorial-intent inquiry is used as a balancing tool

65. *Id.* at 530.
66. *Id.*
67. *Id.* at 529–30.
68. *Id.* at 531 (quoting Frank v. Maryland, 359 U.S. 360, 367 (1959)).
69. *Id.*
70. *Id.* at 531–32.
71. *Id.* at 532.
72. *Id.* at 532–33.
73. *See* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 528 (7th Cir. 2018).

to discern the depth of personal interests rather than as a weapon to wholly dismiss community privacy fears.[74]

2. *Naperville* Overlooked the Connection Between Smart Meter Data and Potential Criminal Implications

Although *Camara* dictates a more thorough analysis of privacy interests, some might argue that *Naperville* is properly distinguished since the administrative search in *Camara* had a direct possibility of ending in a criminal citation.[75] Indeed, as the *Naperville* court notes, "using too much electricity is not yet a crime"[76] and the city's Smart Grid Bill of Rights seems to inoculate against any concerns regarding improper usage. However, the crux of *Camara* was that a lack of prosecutorial intent is not conclusive in Fourth Amendment analysis.[77] Moreover, the *Naperville* court itself admitted earlier in its opinion that an inferential step from a nonprosecutorial search to one relating to a criminal proceeding does not render the search outside the scope of the Fourth Amendment's protections.[78]

Further, when viewed in context, the line between the city's platonic use of smart meter data and law enforcement is flimsy. Namely, the city's Smart Grid Bill of Rights is not the emblem of privacy protection that the *Naperville* court makes it out to be.[79] The document itself merely asserts the municipality's intent to protect consumer data[80] but lacks any actual Fourth Amendment implications if the city breaks its own promises. Indeed, the Supreme Court has routinely upheld searches under the Fourth Amendment despite the searches

74. It is important to note that *Camara* was decided in May 1967, whereas *Katz* was decided in December 1967, meaning that *Camara* Court's prosecutorial-intent analysis was not originally designed to be used within the reasonable expectation of privacy test because the test did not exist until half a year later when *Katz* was decided. *See* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (introducing the reasonable expectation of privacy test).

75. *Camara*, 387 U.S. at 531.

76. *Naperville*, 900 F.3d at 528.

77. *See Camara*, 387 U.S. at 530–31 ("[E]ven the most law-abiding citizen has a very tangible interest in limiting the circumstances under which the sanctity of his home may be broken by official authority, for the possibility of criminal entry under the guise of official sanction is a serious threat to personal and family security."); *see also* Maximilian Sladek de la Cal, City of Los Angeles v. Patel*: The Fourth Amendment's "Special Needs" in the Information Age*, 31 BERKELEY TECH. L.J. 1137, 1141 (2016).

78. *Naperville*, 900 F.3d at 526.

79. *Id.* at 528 ("And Naperville's amended 'Smart Grid Customer Bill of Rights' clarifies that the city's public utility will not provide customer data to third parties, including law enforcement, without a warrant or court order. Thus, the privacy interest at stake here is yet more limited than that at issue in *Camara*.").

80. *See* NAPERVILLE, ILL., CODE OF ORDINANCES § 8-0.5-2(2)–(4) (LEXIS through Ordinance No. 21-007).

violating narrower local law.[81] Because the Fourth Amendment functions as a constitutional minimum, Naperville and other cities and states are free to impose additional standards, the violation of which will be irrelevant to a Fourth Amendment inquiry.[82] In this instance, because the Seventh Circuit upheld the city's data collection as a reasonable search under the Fourth Amendment,[83] if future well-intentioned city officials feel compelled to diverge from the Smart Grid Bill of Rights in response to pleas from law enforcement to assist in the conviction of an individual, the Fourth Amendment would be of no assistance to Naperville residents.[84] Instead, the city's decision to leverage their data for criminal purposes would leave customers with no constitutional recourse.

Notably, the previous hypothetical regarding the use of electricity data to convict a person is not a far-fetched example. Electricity consumption data has become increasingly valuable to government agencies for use in criminal prosecutions, particularly in federal drug investigations.[85] For example, heightened electricity usage can indicate that a resident is using high-wattage grow lights to grow marijuana.[86] In fact, law enforcement agencies have explicitly acknowledged the importance of this data for discovering grow operations when traditional investigative methods fail to reveal any evidence of a crime.[87] Strikingly, too, collecting smart meter data typically only requires a subpoena, not a warrant, which means the agency need only have a reasonable belief that criminal activity has occurred, significantly lowering the threshold

81. *See generally* Virginia v. Moore, 553 U.S. 164 (2008) (upholding the conviction of a defendant whose arrest for a suspended driver's license was contrary to state law because the seizure was still reasonable under the Fourth Amendment); Whren v. United States, 517 U.S. 806 (1996) (affirming the reasonableness of a vehicle stop by plainclothes officers in an unmarked car despite D.C. regulations prohibiting these kinds of stops); Cooper v. California, 386 U.S. 58 (1967) (reversing the state court's determination that violation of state law during a vehicle seizure was also a violation of the Fourth Amendment).

82. *See Moore*, 553 U.S. at 171 ("Our decisions counsel against changing [our Fourth Amendment inquiry] when a State chooses to protect privacy beyond the level that the Fourth Amendment requires. We have treated additional protections exclusively as a matter of state law.").

83. *See supra* Section I.B.

84. It takes little imagination to envision a situation in which the local police approach the city with a plea to hand over data under the guise of public safety and the city bending to the wishes of the law enforcement agency.

85. *See, e.g.*, United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1117 (9th Cir. 2012) (sustaining the U.S. Drug Enforcement Administration's subpoena of electricity consumption data from three residents served by an electric cooperative for use in a drug investigation).

86. Dean Narciso, *Police Seek Utility Data for Homes of Marijuana-Growing Suspects*, COLUMBUS DISPATCH (Feb. 28, 2011, 12:01 AM), https://www.dispatch.com/article/20110228/news/302289766 [https://perma.cc/BQ5D-7KS7].

87. *Id.*

for the government.[88] One investigator even recognized the increasing value of smart meter data specifically for its ability to provide details traditionally unknown to police outside a warrant—"How else can I get an indicator to get probable cause if I can't see anything?"[89] In effect, smart meter data allows government agencies to turn mere hunches about criminal activity into full-blown investigations. These tactics are not foolproof either—innocuous, noncriminal activity can also be implicated in these searches. In 2011, a federal investigator revealed to state law enforcement that what the detectives believed to be a "major grow operation" based off of utility records actually ended up being a man's at-home business involving numerous high-wattage computer servers.[90]

Importantly, these are not obscure policing strategies. In 2011, at least sixty subpoenas per month were filed in Ohio requesting energy-use records from residents.[91] More recently, in 2017, Pacific Gas & Electric ("PG&E"), the country's largest utility,[92] received 343 demands from legal entities for customer data records that covered approximately 125,800 residents.[93] Although PG&E is a privately owned utility (in contrast to government-owned utilities like the one in *Naperville*) and requires a warrant to access the data,[94] these examples highlight the burgeoning demand for information. Moreover, the growing requests for smart meter data provide significant opportunities for abuse in government-owned utilities when there is no barrier between electricity consumption data and unfettered government access—because the utility company and the government are part of the *same* entity. Thus, not only is there a plausible connection between smart meter data and criminal implications, but the government is also already weaponizing this essential

88. *See* Murphy, *supra* note 30, at 801–03 (describing instances of law enforcement using subpoenas to gather electricity consumption data); *id.* at 799–800 ("An important distinction between subpoenas and warrants is that warrants always require a showing of probable cause, whereas subpoenas require a lower burden of proof."); *see also* United States v. R. Enters., Inc., 498 U.S. 292, 297 (1991) ("[T]he very purpose of requesting the information [via subpoena] is to ascertain whether probable cause exists."); *Golden Valley*, 689 F.3d at 1113–14 ("We 'must enforce administrative subpoenas unless the evidence sought by the subpoena is plainly incompetent or irrelevant to any lawful purpose of the agency.'" (quoting EEOC v. Karuk Tribe Hous. Auth., 260 F.3d 1071, 1076 (9th Cir. 2001))).

89. Narciso, *supra* note 86.

90. *Id.*

91. *Id.*

92. *The 5 Largest Utilities in the U.S.*, SAVEONENERGY (Jan. 31, 2020), https://www.saveonenergy.com/learning-center/post/top-5-utilities-in-u-s/ [https://perma.cc/5Y62-64BV].

93. PAC. GAS & ELEC. CO., SMART GRID ANNUAL PRIVACY REPORT 2017, at tbl.1 (2017), https://www.cpuc.ca.gov/General.aspx?id=6442457990 [https://perma.cc/5L3L-6JBH] (choose "2017" from "PG&E").

94. *Notice of Accessing, Collecting Storing, Using and Disclosing Energy Usage Information*, PG&E, https://www.pge.com/en_US/about-pge/company-information/privacy-policy/energy-usage-information/energy-usage-information.page [https://perma.cc/XS34-JDB9] (last updated Jan. 1, 2020).

service against individuals whose only method of avoiding monitoring would be to live off the grid entirely.

B. *Turning the Lights On: A Proper Analysis of Individual Privacy Interests in Smart Meter Data*

In addition to its failure to approach smart meter data in a contextualized manner, the *Naperville* court relied solely on its prosecutorial-intent inquiry in reasoning that customers had diminished privacy interests.[95] It conducted no analysis into the intrusiveness of the search, whereas Fourth Amendment precedent is ripe with analogous technological search examples, all of which are objectively less intrusive than smart meter data and pose less risk to individuals in terms of the information they can provide the government. For example, *United States v. Karo*[96] found that the use of electronic "beepers" on a shipment of supplies that then entered a private residence violated the privacy interests of those inside.[97] Similarly, *Kyllo v. United States*[98] concluded that the use of thermal-imaging devices on a private residence that provided "relatively crude"[99] heat imagery was an unreasonable search.[100] *Riley v. California*[101] even established that text messages, call logs, photos, and videos contained on a cell phone collected after a lawful physical search could not be examined absent a warrant.[102] All of these technological examples would have provided government entities with significantly less granular information than smart meters, but all of them were deemed unreasonable because of the privacy principles implicated.

Even more striking, under the *Katz* reasonable expectation of privacy test, the Supreme Court has come to recognize that as technology becomes ingrained into every crevice of our lives, the Fourth Amendment must accommodate the reality that individuals are often helpless to live their lives without it. *Carpenter v. United States*[103] is enigmatic of this principle. In *Carpenter*, the Supreme Court held that the defendant had a reasonable expectation of privacy in cell-site location information ("CSLI") furnished by his cell phone carrier to the government that included "12,898 location points cataloging Carpenter's

95. Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 528 (7th Cir. 2018).
96. 468 U.S. 705 (1984).
97. *Id.* at 717.
98. 533 U.S. 27 (2001).
99. *Naperville*, 900 F.3d at 526.
100. *Kyllo*, 533 U.S. at 40.
101. 573 U.S. 373 (2014).
102. *See id.* at 401.
103. 138 S. Ct. 2206 (2018).

movements over 127 days" without a warrant.[104] For the Court, the fact that Carpenter had, in effect, surrendered this information to his cell phone provider was irrelevant because "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[105] Cell phones are now in essence a "feature of human anatomy," and the Supreme Court recognized the need to account for their pervasiveness.[106]

If cell phones are categorized as essential to modern life under *Carpenter*, then electricity is undoubtedly even more indispensable to present-day living because cell phones themselves are reliant on electricity. Further, the first iPhone was released in 2007,[107] whereas Thomas Edison patented the incandescent lightbulb in 1880,[108] and the level at which each is embedded into everyday life is similarly disparate. While life would be incredibly inconvenient without a cell phone, a single day without electricity would place the health and safety of millions of individuals in jeopardy. Life-saving medical devices,[109] refrigeration,[110] heating and air conditioning,[111] and numerous other technologies that provide for essential human activity are dependent on reliable electricity. One need to only look to the devastating consequences imposed by power outages during extreme weather events to fully comprehend the degree

104. *Id.* at 2209, 2219. Cell-site location information can provide the government with a detailed account of where an individual was located at specific times because "[e]ach time the phone connects to a cell site, it generates a time-stamped record." *Id.* at 2211. Most cell phones "tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features." *Id.*

105. *Id.* at 2210 (quoting *Riley*, 573 U.S. at 385).

106. *Riley*, 573 U.S. at 385.

107. *Steve Jobs Debuts the iPhone*, HISTORY, https://www.history.com/this-day-in-history/steve-jobs-debuts-the-iphone [https://perma.cc/CX5Q-FM8X] (Jan. 7, 2020).

108. *History of Electricity*, INST. FOR ENERGY RSCH., https://www.instituteforenergyresearch.org/history-electricity/ [https://perma.cc/2PD7-PJXW].

109. *See* PAC. ADA CTR., EMERGENCY POWER PLANNING FOR PEOPLE WHO USE ELECTRICITY AND BATTERY DEPENDENT ASSISTIVE TECHNOLOGY AND MEDICAL DEVICES 1 (2014), https://www.pge.com/pge_global/common/pdfs/safety/electrical-safety/electric-generator-safety/Pacific-ADA-Centers-Emergency-Power-Planning-Fact-Sheet.pdf [https://perma.cc/Q5QS-QNFC] (providing an emergency preparedness checklist for individuals who use essential medical devices in their homes in case of a power outage).

110. *See Food Safety for Power Outages*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/foodsafety/food-safety-during-a-power-outage.html [https://perma.cc/7AYG-PAMB] (last updated Sept. 8, 2020) (providing guidance for how to determine whether refrigerated food is unsafe after a power outage).

111. *See Hot Weather Safety for Older Adults*, U.S. DEP'T HEALTH & HUM. SERVS.: NAT'L INST. ON AGING, https://www.nia.nih.gov/health/hot-weather-safety-older-adults [https://perma.cc/R2VF-78D9] (last updated June 15, 2016) (listing potential health consequences for elderly people who are exposed to extreme heat conditions during warm-weather months).

to which human life depends on it.[112] Under this perspective, the need for electricity is undeniable, and absent additional governmental protections, people are forced to choose between living in a modern society or safeguarding their most private moments—a balancing that the Court repudiated in *Carpenter*.[113] Further, the data collection in *Naperville* poses an even greater risk to individuals than the CSLI data collection in *Carpenter*, simply because it is the government itself that collects it—not a disinterested third party.[114] Thus, as in *Carpenter*, courts must recognize that the data generated by electric meters, which sustains basic human functions, should be properly shielded from the government under the traditional warrant machinery.

IV. AN APPROPRIATE FOURTH AMENDMENT ANALYSIS REQUIRES CONSIDERATION OF THE LOCATION AND NATURE OF THE SEARCH

In anchoring its reasonableness conclusions on the lack of prosecutorial intent, the Seventh Circuit deflected in its duty to examine the significant privacy interests implicated in smart meter data collection. Specifically, it downplayed two critical aspects of the data collection—its use within the home and the longitudinal nature of the search. The following sections explore each in turn.

A. Naperville *Failed To Address the Significance of Searches Within the Home*

Naperville's reasonableness assessment most prominently omits any mention of the critical fact that the city's smart meter data is collected from a person's private residence. In Fourth Amendment jurisprudence, "the home is first among equals"[115] and the private affairs of an individual within the home are granted unparalleled deference.[116] The *Naperville* court correctly identifies

112. *See* Shawn Mulcahy, *Many Texans Have Died Because of the Winter Storm. Just How Many Won't Be Known for Weeks or Months*, TEX. TRIB. (Feb. 19, 2021), https://www.texastribune.org/2021/02/19/texas-power-outage-winter-storm-deaths/ [https://perma.cc/RYH3-7TZR] (describing a variety of causes of death linked to Texas power outages including hypothermia and carbon monoxide poisoning); N'dea Yancey-Bragg, *Family Suing Texas Utility Companies for $100M After 11-Year-old Boy Died Amid Power Failure*, USA TODAY (Feb. 22, 2021), https://www.usatoday.com/story/news/nation/2021/02/22/family-sues-ercot-entergy-boys-death-texas-power-outages/4538181001/ [https://perma.cc/EPU5-2SQF] (detailing the plight of parents whose son died of suspected hypothermia during a Texas power outage).

113. *Cf.* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements." (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979))).

114. McGovern, *supra* note 32 ("[T]hese [utility] companies aren't doing anything other than reading your meter and providing you with the best service that they can. They also encrypt all of the data that is transmitted to and from these smart meters, making it difficult for third parties to access the information without consent.").

115. Florida v. Jardines, 569 U.S. 1, 6 (2013).

116. Anna Lvovsky, *Fourth Amendment Moralism*, 166 U. PA. L. REV. 1189, 1213–15 (2018).

that electric smart meter data is collected without prosecutorial intent, which, in the court's view, lessens the significance of the intrusion.[117] However, it is equally, if not more important, that the search is conducted within the home—the most revered space in Fourth Amendment analysis. "The unpermitted entry into the household, the Court has declared, 'is the chief evil against which the wording of the Fourth Amendment is directed.'"[118]

Unwarranted intrusions into the home are not only a significant oppression prohibited by the Fourth Amendment but arguably the *central* tenet around which its jurisprudence has been crafted. Indeed, "[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from governmental intrusion."[119] The protection of the home is so fundamental to the Fourth Amendment that "[w]ith few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no."[120] The primacy of the home is further highlighted in Fourth Amendment privacy cases where the reasonableness of an individual's privacy interest in a particular space, whether the "curtilage" of their home[121] or within a business operation,[122] is gauged in reference to how similar the space is to an individual's home. For example, in *Oliver v. United States*,[123] the Supreme Court established that "[t]here is no societal interest" in respecting the privacy interests of those who conduct activities on privately owned "open fields" because expectations of privacy while cultivating crops are significantly different from expectations of privacy for "intimate activity" within the home.[124] In contrast, the Court in *Florida v. Jardines*[125] held that the use of drug-sniffing dogs on the front porch of the defendant's house was a violation of the defendant's reasonable expectation of privacy because "[t]he area 'immediately surrounding and associated with the home' . . . . is 'intimately linked to the home, both physically and psychologically.'"[126]

Notably, the home has been revered as a sacred space, not solely in reference to an individual's right to exclude others as a function of privacy and familial life, but as a reflection of an individual's "unique property and sovereignty interests."[127] Thus, an individual's right to maintain a home free

117. *See supra* Section III.A.

118. Lvovsky, *supra* note 116, at 1212 (quoting United States v. U.S. Dist. Ct., 407 U.S. 297, 313 (1972)).

119. Silverman v. United States, 365 U.S. 505, 511 (1961).

120. Kyllo v. United States, 533 U.S. 27, 31 (2001).

121. *See* United States v. Dunn, 480 U.S. 294, 300 (1987).

122. *See* New York v. Burger, 482 U.S. 691, 700 (1987).

123. 466 U.S. 170 (1984).

124. *Id.* at 179–80.

125. 569 U.S. 1 (2013).

126. *Id.* (first quoting Oliver v. United States, 446 U.S. 170, 180 (1984); and then quoting California v. Ciraolo, 476 U.S. 207, 213 (1986)).

127. Lvovsky, *supra* note 116, at 1213.

from governmental invasion is inherent to their citizenry.[128] Because the sanctity of the home is so fiercely protected in Fourth Amendment jurisprudence and is deeply embedded in American society as a fundamental piece of identity, it is anomalous that *Naperville* made no assessment of it while balancing individuals' privacy rights against governmental interests.

B. Naperville *Overlooked How Longitudinal Data Collection Heightens Privacy Concerns*

In addition to its failure to consider the primacy of the home in Fourth Amendment jurisprudence, the *Naperville* court further departed from settled legal principles by asserting that smart meter data collection "is far less invasive than the prototypical Fourth Amendment search of a home."[129] In doing so, it failed to consider that longitudinal data collection compounds the intrusiveness of a search. With this omission, the *Naperville* court fatally downplayed the customers' interest in privacy.

As in *Jones*, the *Naperville* data collection constitutes a longitudinal search. Because every electricity-consuming device in our homes produces a unique load signature,[130] a person examining the data can discern not only what time an individual took a shower or washed their dishes on a particular day, but also the time at which an individual has taken a shower every single day for the past year and what brand of electric water heater they use.[131] Moreover, in controlled experiments, it has also been shown that smart meter data can reveal not only *when* a resident was watching television but also *what* they were watching.[132] A prototypical Fourth Amendment search presents a snapshot in time of an individual's private residence, belongings, or self, whereas electric smart meter data provides a vivid, detailed account of an individual's regular habits.[133] Thus, the *Naperville* court's assertion that the data collection is "far less invasive"[134] is directly contrary to the findings in *Jones*. In fact, the *Naperville* search is arguably *even more invasive* than the *Jones* search because it provides specific details as to the activities of those it monitors,[135] whereas the *Jones* search provided only locational data.[136]

128. *See id.*

129. Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 528 (7th Cir. 2018).

130. *See supra* Section II.A.

131. *See Naperville*, 900 F.3d at 526; *supra* Section II.A.

132. *See* ULRICH GREVELER, PETER GLÖSEKÖTTER, BENJAMIN JUSTUS & DENNIS LOEHR, MULTIMEDIA CONTENT IDENTIFICATION THROUGH SMART METER POWER USAGE PROFILES 4 fig.5, https://1lab.de/pub/ike2012.pdf [https://perma.cc/HPV3-AM78] (demonstrating the unique power-consumption data for movies such as *Star Trek* and *Body of Lies*).

133. *Naperville*, 900 F.3d at 526.

134. *Id.* at 528.

135. *See supra* Section II.A.

136. United States v. Jones, 565 U.S. 400, 402 (2012).

In addition, the *Naperville* court made the distinction between electricity consumption data and other searches by noting that the use of smart meters is not a physical intrusion into someone's home.[137] This is a false equivalency. The assertion that electronic surveillance tools—which can reveal intimate details of an individual's home—are less intrusive than physically entering an individual's house is not supported by the Supreme Court's Fourth Amendment jurisprudence. Indeed, under this flawed logic, all uses of technology would be immune to the Fourth Amendment simply because they do not require a physical entrance into a building—a conclusion wholly unsupported by the Supreme Court's Fourth Amendment jurisprudence.[138] Instead, the Supreme Court has explicitly stated that "property rights are not the sole measure of Fourth Amendment violations."[139] In *Jones*, Justice Sotomayor even asserted that the physical trespassory test constitutes "an irreducible constitutional minimum."[140] Thus, the physical invasion requirement is merely the floor, not the ceiling, and reducing Fourth Amendment searches to only cover physical invasions is "highly artificial."[141] Moreover, the *Katz* reasonable expectation of privacy test indicates that the reasonableness of a search is gauged by *what* information is garnered by it and *where* it occurred, not the method in which it was conducted.[142] The Seventh Circuit's rigid construction of the Fourth Amendment is exactly what the Supreme Court has fought against because it "leave[s] the homeowner at the mercy of advancing technology."[143]

Had the *Naperville* court proceeded in an appropriate analysis, it would have found that smart meter data collection is the functional equivalent of a physical entry into a resident's private residence and therefore warranted a more thorough inquiry into the privacy risks it imposed on every resident in the City of Naperville. Moreover, as a passive search, data collection generally poses even more serious privacy risks to individuals because it is "detailed,

137. *Naperville*, 900 F.3d at 528 (noting that the search in *Camara* was distinct because physical entry into a home constitutes a "serious threat to personal and family security" (quoting Camara v. Mun. Ct. of S.F., 387 U.S. 523, 531 (1967))).

138. *See* Carpenter v. United States, 138 S. Ct. 2206, 2214 n.1 (2018) ("But while property rights are often informative, our cases by no means suggest that an interest is 'fundamental' or 'dispositive' in determining which expectations of privacy are legitimate.").

139. Soldal v. Cook County, 506 U.S. 56, 64 (1992).

140. *Jones*, 565 U.S. at 414 (Sotomayor, J., concurring).

141. *Id.* at 418–19 (Alito, J., concurring) (arguing that the majority's use of eighteenth-century tort law to determine the unreasonableness of a search was outdated).

142. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (arguing that reasonableness is gauged by an individual's expectation of privacy in regard to "objects, activities, or statements," and when those exist outside an area that society reasonably respects as private, they are not protected).

143. Kyllo v. United States, 533 U.S. 27, 35 (2001) (explaining that the use of a thermal-imaging device could not avoid classification as a search simply because it collected "off-the-wall" rather than "through-the-wall" information).

encyclopedic, and effortlessly compiled."[144] Electronic data collection is dangerous for precisely the reason that *Naperville* dismissed it as a minor invasion—it provides information otherwise unknowable via a traditional search.[145] This leaves greater potential for abuse by government officials[146] and conjures images of a surveillance state, the result of "the dystopian vision of Orwell or Huxley."[147]

Compounding these oversights—the significance of the search being conducted in the home and the intrusiveness of aggregate data collection—the *Naperville* court deflected the opportunity to draw a bright-line rule in favor of privacy rights within our increasingly digitized society.

V. FOURTH AMENDMENT PRIVACY PRINCIPLES REQUIRE SMART METER DATA TO REMAIN PRESUMPTIVELY OFF-LIMITS TO THE GOVERNMENT

Courts are quick to defer the complex task of creating a concrete Fourth Amendment electronic-privacy framework to others. Namely, the Supreme Court has asserted that legislative bodies are best equipped to address privacy concerns that emerge from electronic monitoring devices.[148] Similarly, the *Naperville* court rested its reasonableness determination on the fact that the municipal utility had a Smart Grid Bill of Rights requiring that local law enforcement acquire a warrant prior to accessing the data.[149] In addition, the Seventh Circuit limited its conclusion to the specific facts laid out before it.[150] It asserted that data collection at more frequent intervals might necessitate a different conclusion[151] and even opined that the utility could circumvent future privacy issues by allowing customers to opt in to the smart meter program.[152]

Obviously, courts are limited to solely adjudicating the cases before them and venturing into hypotheticals would be appropriately considered judicial activism. However, the fundamental right to privacy has been established as within the judiciary's purview for generations via the "penumbra" found within

144. Carpenter v. United States, 138 S. Ct. 2206, 2209 (2018).

145. Sladek de la Cal, *supra* note 77, at 1138.

146. *Id.* at 1138–39.

147. R. Reeve Wood III, *The Prolonged Arm of the Law: Fourth Amendment Principles, the* Maynard *Decision, and the Need for a New Warrant for Electronic Tracking*, 64 ME. L. REV. 285, 299 (2011).

148. United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring).

149. Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 528 (7th Cir. 2018); *see also* NAPERVILLE, ILL., CODE OF ORDINANCES § 8-0.5-2(2)(E) (LEXIS through Ordinance No. 21-007). Notably however, the court does not venture into determining whether it would have required a warrant absent the Smart Grid Bill of Rights.

150. *Naperville*, 900 F.3d at 529.

151. *Id.* It is also striking that while the court's conclusion hinges on the fifteen-minute interval of the search, there is no mention of frequency of the data collection within its reasonableness assessment. *Id.* at 527–28.

152. *Id.* at 529.

the U.S. Bill of Rights.[153] The invasive nature of smart meter data and its potential to significantly diminish privacy rights requires a bright-line Fourth Amendment rule.

Moreover, the current Fourth Amendment privacy framework encourages judges to make value judgments—what is society willing to recognize as so fundamental as to be entirely off-limits by intrusion from the government?[154] In light of this, the current judicial hesitance to create a concrete privacy rule in reference to certain technology due to fears of the changing social and technological landscape is certainly misplaced, as the reasonable expectation of privacy test already mandates that courts make normative claims involving technology.[155]

Under these background principles, the data garnered from electric smart meters is so deeply intimate and personal that it requires a Fourth Amendment rule excluding smart meter data from collection by the government absent a warrant or consent. This means that investor-owned utilities and electric cooperatives will be required to keep electricity-consumption data private absent express permission of individual customers, and that publicly owned utilities,[156] such as the one in *Naperville*, will need to find an alternate method of collecting consumption data or include an opt-out provision.[157] Importantly, there are viable alternative methods to collecting the granular data that do not jeopardize efficiency benefits. Government-run utilities can store their data off site via a third party[158]or leverage aggregation tools which anonymize the data

153. Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965).

154. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also* Lvovsky, *supra* note 116, at 1209.

155. Lvovsky, *supra* note 116, at 1212.

156. It is particularly relevant to emphasize that only about fifteen percent of utility customers across the country are served by publicly owned utilities. *See Investor-Owned Utilities Served 72% of U.S. Electricity Customers in 2017*, U.S. ENERGY INFO. ADMIN.: TODAY ENERGY (Aug. 15, 2019), https://www.eia.gov/todayinenergy/detail.php?id=40913 [https://perma.cc/J5ER-T68T]. Thus, a requirement that publicly owned utilities use an alternative method for data collection would not significantly impact the majority of Americans or utility companies, diminishing any argument in reference to the administrative burden of implementing such a rule.

157. There are numerous alternative methods of collecting load data that do not sacrifice grid modernization efforts. Some of these include the anonymization or aggregation of data, *see generally* FÁBIO BORGES DE OLIVEIRA, ON PRIVACY-PRESERVING PROTOCOLS FOR SMART METERING SYSTEMS: SECURITY AND PRIVACY IN SMART GRIDS (2017) (describing numerous privacy-protecting protocols that ensure consumption data are anonymized), or storing the data off site via a third party, *see* Coley Girouard, *Advanced Metering: Making the Most of Connectivity for a Modern Grid*, UTIL. DIVE (Sept. 20, 2017), https://www.utilitydive.com/news/advanced-metering-making-the-most-of-connectivity-for-a-modern-grid/505283/ [https://perma.cc/26ZQ-MAES].

158. *See* Hajer Souri, Amine Dhraief, Syrine Tlili, Khalil Drira & Abdelfettah Belghith, *Smart Meter Privacy-Preserving Techniques in a Nutshell*, 32 PROCEDIA COMPUT. SCI. 1087, 1092 (2014) ("[W]e often resort to a third party that we consider as trustworthy.").

without sacrificing its value to the utility.[159] Thus, the central purpose of smart meters is left intact, while privacy concerns are appropriately managed.

Critics might assert that a sweeping ban on this type of data collection can lead to a slippery slope in which government agencies, such as the City of Naperville's utility, are required to operate using obsolete technologies to avoid infringing on wide-sweeping privacy rights. This is a particularly salient consideration, as few might consider their electric utility company a major threat to their personal autonomy or freedom from government overreach. However, the inherent purpose of privacy concerns within the Fourth Amendment is to address the slippery slope problem—but in the other direction: "Privacy violations can train violators to depersonalize and dehumanize the individuals with whom they deal, and those are particularly dangerous habits and ways of thinking for governmental officers and agencies, because of the tools of coercion and violence they can lawfully employ."[160] In reality, establishing a bright-line ban on warrantless, nonconsensual collections of electricity consumption data staves off this problem—an absolute prohibition evades the shades-of-gray assessment that courts engage in when determining what time interval, or what level of access, tips such collection into an unreasonable search.

Another potential criticism of an explicit warrant requirement is that it would inhibit effective policing. One might argue that only those who commit crimes in their homes should have any substantive fear of smart meter data collection. However, a warrant requirement does not keep government agencies from accessing these data—it just requires they demonstrate to a neutral, detached magistrate that they have probable cause.[161] At its heart, the warrant requirement "is concerned with government power and its abuse, and a warrant requirement built on specificity and limited discretion is the means by which we have chosen to prevent such abuse."[162] Moreover, the Court has repudiated the concerns that warrants are unduly burdensome in nonemergency situations. In *Johnson v. United States*,[163] police received a confidential tip that the defendant was using narcotics in his hotel room and upon arrival to the room could smell "burning opium."[164] Acting on the tip and odor, police entered the room, confronted the occupants, and conducted a search.[165] The Supreme Court

159. *Id.*
160. Sklansky, *supra* note 5, at 1113.
161. Johnson v. United States, 333 U.S. 10, 13–14 (1948).
162. Wood, *supra* note 147, at 292.
163. 333 U.S. 10 (1948).
164. *Id.* at 12.
165. *Id.*

sharply rebuked the officers for failing to request a warrant prior to entry.[166] In its opinion, the Court stated:

> The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.[167]

Moreover, the assumption that only criminals need be concerned about an overreaching government with unrestricted access to our homes contains a misguided view of the accuracy of policing. The sheer amount of wrongfully convicted individuals across the country attests to the strong possibility that evidence collected against innocent individuals can, and is, still being weaponized to convict them. Since 1989, 2,720 individuals have been exonerated of crimes in the United States.[168] Of these individuals, 663 of these false convictions had been at least partly based on false or misleading forensic evidence,[169] and 1,488 were convicted based on official misconduct, such as failure by the police or prosecutor to release exculpatory evidence to the defense.[170] Although police are not directly responsible for convictions, their work is critical to any conviction, and their policing tactics directly impact the availability of reliable evidence that leads to criminal charges. Recognizing that police agencies are composed of human beings capable of error, a warrant requirement adds an additional layer of protection and serves the Fourth Amendment purpose of "plac[ing] obstacles in the way of a too permeating police surveillance."[171]

Finally, it is important to note that the *Naperville* court was correct in its assessment of the government's heightened need for smart meter data. Grid modernization efforts, as well as climate change goals, are heavily dependent on

166. *See id.* at 13–14 ("When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or government enforcement agent.").

167. *Id.*

168. *Exonerations in the United States Map*, NAT'L REGISTRY EXONERATIONS, http://www.law.umich.edu/special/exoneration/Pages/Exonerations-in-the-United-States-Map.aspx [https://perma.cc/C4MN-M5VC] (last updated Jan. 26, 2021) (featuring an interactive map that tracks known exonerations in the United States since 1989).

169. *Id.* (choose "Present" for "Bad Forensic Evidence" under the "Contributing Factors" section).

170. *Id.* (choose "Present" for "Official Misconduct" under the "Contributing Factors" section); MARC ALLEN, NON-*BRADY* LEGAL AND ETHICAL OBLIGATIONS ON PROSECUTORS TO DISCLOSE EXCULPATORY EVIDENCE (2018), http://www.law.umich.edu/special/exoneration/Documents/NRE_Exculpatory_Evidence_Obligations_for_Prosecutors.pdf [https://perma.cc/GED8-Q3M9] ("In addition to constitutional constraints, prosecutors and police may also be bound by ethics rules, statutes, professional standards, and court rules.").

171. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

granular consumption data, allowing utilities to better prepare for weather-related disruptions, prevent blackouts, adopt renewable technologies, and provide consumers with access to their own usage to facilitate efficiency efforts.[172] However, just as society understands that restricting use of other surveillance tools in the Fourth Amendment context does not compromise legitimate law enforcement or administrative agency goals, [173] grid modernization efforts and the use of smart meter installations are not mutually exclusive with ensuring adequate privacy and Fourth Amendment guarantees. Technology is adaptable to constitutional mandates, but fundamental rights are inalienable.[174]

CONCLUSION

The *Naperville* court departed from well-established Fourth Amendment privacy principles in its analysis of electric smart meters. Critical attributes of the data collection, including the collection's longitudinal nature and the fact that the data captured intimate details from within the home, were entirely overlooked.[175] The singular axis of analysis along which the court determined the validity of the search was that the search was conducted without prosecutorial intent. In the court's view, this lack of intent heavily tipped the scales in favor of the government.[176] This flawed analysis led to an outcome that poses significant threats to personal privacy in a data-dependent country.

The Fourth Amendment has evolved from a property-based theory rooted in tangible concepts of tort and trespass[177] to now account for searches that invade our most intimate spaces and deny us our sense of autonomy from the government.[178] This evolution in the Fourth Amendment is a reflection of a greater technological revolution in which the government can search us and seize our property without a physical intrusion into our most protected spaces.[179] Had the *Naperville* court properly assessed the interests of individuals in their privacy, it would have had to confront the ways in which smart meter data collection poses a substantial threat to privacy within the home—the most sacred space within Fourth Amendment jurisprudence. Properly addressing the data collection as a significant privacy intrusion would have necessitated that the court create a bright-line rule in regard to smart meter data collection.

172. *See* SMART GRID SYSTEM REPORT, *supra* note 33, at 22–27.

173. *See supra* notes 155–65 and accompanying text.

174. Christopher Slobogin, *A Defense of Privacy as the Central Value Protected by the Fourth Amendment's Prohibition on Unreasonable Searches*, 48 TEX. TECH L. REV. 143, 158 (2015).

175. *See supra* Part IV.

176. Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 528–29 (7th Cir. 2018).

177. *See* United States v. Jones, 565 U.S. 400, 404–05 (2012).

178. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

179. *See* Sklansky, *supra* note 58, at 1119.

This Recent Development proposes that the solution to electric smart meter data is an unambiguous Fourth Amendment rule prohibiting data collection that provides granular, individualized information about residents absent a warrant or consent. This would require government-owned utilities to outsource their data collection, leverage anonymization tools, or utilize other technological resources to ensure appropriate data privacy safeguards.[180] These efforts will require forward-thinking leadership but need not inhibit grid modernization goals—a key factor in the court's decision in *Naperville*.[181]

ALEXANDRA FRANKLIN[**]

180. *See supra* note 157 and accompanying text.

181. *Naperville*, 900 F.3d at 529.

** I would like to thank my primary editor Nicholas Gallo for his dedication to this Recent Development throughout the publication process and for sharing my sentiment regarding the importance of Fourth Amendment privacy rights. And to my family, I am incredibly grateful for your unwavering support of all of my academic pursuits.