PROTECTING ENERGY PRIVACY ACROSS THE PUBLIC/PRIVATE DIVIDE

Matthew B. Kugler & Meredith Hurley[*]

Abstract

Energy-usage monitoring can expose much of what takes place inside people's homes and offices. As the "smart home" revolution continues, this data will only become more revealing. Though this information is essential for the development of the smart electric grid, it is also useful to a variety of others: law enforcement, energy-efficiency experts, and marketers. At present, this data enjoys little Fourth Amendment or statutory protection. This was not previously a problem because the information was historically not overly sensitive. Now that utilities are collecting more than two thousand times as much information about households as they were before, however, more protection is needed. This Article traces the rise of "smart meter" technology, evaluates the Fourth Amendment implications of law enforcement access to smart meter records, and proposes a statutory framework to govern public and private access to such data. It also reflects on the growing challenge of protecting digital privacy in an era where once undetectable information is now readily and involuntarily shared with third parties and on the Fourth Amendment implications of failing to restrict private use of sensitive data.

---

* Matthew B. Kugler is an Associate Professor at Northwestern University Pritzker School of Law. Meredith Hurley is a recent graduate of Northwestern University Pritzker School of Law. The Authors thank Zachary Clopton, Charlotte Crane, John McGinnis, Janice Nadler, Laura Pedraza-Farina, James Pfander, David Schwartz, Nadav Shoked, James Speta, and Matthew Spitzer for their comments on earlier versions of this Article; workshop participants at ETH Zürich for their helpful feedback; and Miranda Roberts for her research assistance.

> At the [Fourth Amendment's] very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.[1]

INTRODUCTION

As cellular location data show what you do outside the home, energy-usage data show what you do inside of it. Recent changes in how energy-usage data is collected and analyzed have drastically altered how much can be inferred from this once innocuous information. This change in information intrusiveness requires a similar change in information protection. This Article sets out a proposal for enhanced energy privacy, calling for an expansion of Fourth Amendment protections and new federal regulations.

To understand why this data is important, think about how the energy usage of a given house might fluctuate from midnight to midnight. At 1 AM, energy usage dips as the dishwasher and clothes dryer set to run before the occupants went to bed finish their preprogrammed cycles. At 5:50 AM, a sharp but brief surge signals the activation of a coffeemaker bringing water rapidly to boil. At 6:03 AM, there is a slight rise as lights begin to turn on. At 6:15 AM, the electric water heater begins a new cycle; someone is showering. The data progress onwards to the dip in usage when the last occupant leaves the house for the day, to the steady rise as person after person returns home after work or school, to again a decline in the evening as people move gradually toward bed. The data look harmless at first, but the patterns rapidly become clear. This regular cycling is the furnace, refrigerator, or air conditioner. That sharp spike is a hair dryer or electric kettle. Soon it becomes possible to tell stories—the house is empty at one time and full at another. A weekday in this house follows this rhythm. A weekend follows a different one. This weekend? The occupants hosted a party. That weekend? They came home late every night. All this data is neatly recorded and stored.

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

This kind of granular energy-usage data can now be routinely collected and shared with local utilities by "smart meters."[2] This collection brings with it many benefits, but it comes at a real privacy cost. Normally, it would leave no trace you were home alone, watching TV. It is the archetypal bad alibi. But energy-usage data provides new opportunities. Was the power usage of your house consistent with someone being home at 7 PM, or did energy consumption only begin to rise hours later? Was there a short spike to indicate that a 1200-watt microwave set to work on a bag of Orville Redenbacher popcorn? The proposed alibi is now testable. Police have already pursued a homicide suspect based in part on smart meter data showing unusual late-night water usage, which they believed suggested the cleanup of a crime scene.[3]

Some might think this is great: now the government can easily determine when you are at home. This will make it easier to investigate crimes and serve warrants. But even if that seems unproblematic, how readily should this data be shared? Should it be available to university researchers looking for potential energy-efficiency improvements? Local department stores hoping to sell you a more efficient clothes dryer? Low-level government employees who may also be your neighbors? Tech companies looking to improve the efficiency and "smartness" of your home?

Many products of the "smart home" revolution pose substantial privacy risks. People buying an Amazon Alexa or Google Home are effectively paying for the privilege of installing microphones and recorders in their own houses.[4] But smart meters are a unique kind of privacy threat. They are involuntarily installed by governmental or quasi-governmental actors: your local utilities. You often cannot simply choose not to have one installed. And they blur the line between public and private surveillance, as the relationship between your utility and the

---

2. *See infra* Section I.B.

3. Affidavit of Probable Cause to Obtain an Arrest Warrant, Arkansas v. Bates, No. CR20160370 (Ark. Cir. Feb. 22, 2016), 2016 WL 7587396. The police affidavit for probable cause supporting the arrest warrant noted that the smart water meters in Bentonville take hourly measurements of electricity and water. *See id.* The data from the smart meter revealed that on the night of the murder, between 1:00 AM and 3:00 AM, the suspect's residence used 140 gallons of water. *Id.* The affidavit asserted that the amount of water used during that time period was consistent with spraying down the back-patio area to clean off blood. *Id.* "Upon reviewing all water usage information, since October 2013 at James' residence, this excessive amount of water usage between [1:00 AM and 3:00 AM] had never before occurred." *Id.* Charges were later dropped. *E.g.*, Colin Dwyer, *Arkansas Prosecutors Drop Murder Case That Hinged on Evidence from Amazon Echo*, NPR (Nov. 29, 2017, 5:42 PM), https://www.npr.org/sections/thetwo-way/2017/11/29/567305812/arkansas-prosecutors-drop-murder-case-that-hinged-on-evidence-from-amazon-echo [https://perma.cc/9EGF-2K7S].

4. *See* Scott Carey, *Does Amazon Alexa or Google Home Listen to My Conversations?*, TECHWORLD (May 25, 2018), https://www.techworld.com/security/does-amazon-alexa-listen-to-my-conversations-3661967/ [https://perma.cc/PJL8-FYVQ].

government is fundamentally determined by history and geography rather than something that you can choose.[5]

Home energy-usage information was historically of limited use. Analog meters were only read once a month (and sometimes not that often), so they did not reveal much beyond whether the occupant was a real energy hog.[6] But now digital smart meters can be read every hour, every quarter hour, or even every five minutes, and there is no great barrier to more frequent measurements.[7] This allows for the disaggregation of energy signatures—turning coarse electricity-usage data into a rich narrative of devices switching on and off. The level of granularity described in the first paragraph is still difficult to see—though achievable if the meter is collecting minute-by-minute data—but that may change over time.[8] A smart meter can link to other devices in the home.[9] Connect a smart meter to a smart home's management hub—which in turn is able to sync with all the smart devices in the household—and the meter will know exactly what some of the big appliances in the home are doing. This will explain much of the home's energy usage, leaving the remaining fluctuations easier to process.

Right now, society is in a transitional period. Smart meters have been installed in much of the country and will only be expanding their reach in the future. But algorithms and tie-in products for smart meters have not yet reached their full potential, so much of their value—both for grid management and for privacy invasion—is in the near future rather than the present. In this way, this Article provides anticipatory recommendations for adequately protecting privacy in the home while also allowing for the development of a more efficient smart home.

Many actors are interested in accessing this energy usage data. Researchers and companies want this information to identify customers, improve product design, and analyze energy consumption.[10] Insurance companies want to monitor whether an insured household is actually

---

5. *See infra* notes 118–119 and accompanying text.

6. *See infra* Section I.A.

7. *See* U.S. DEP'T OF ENERGY, ADVANCED METERING INFRASTRUCTURE AND CUSTOMER SYSTEMS: RESULTS FROM THE SMART GRID INVESTMENT GRANT PROGRAM 10 (2016).

8. *See, e.g.*, Oliver Parson et al., *An Unsupervised Training Method for Non-Intrusive Appliance Load Monitoring*, ARTIFICIAL INTELLIGENCE, Dec. 2014, at 1; *see also infra* notes 95–100 and accompanying text (explaining how information can be extrapolated from smart meter readings).

9. *See infra* Section I.B; *see also Stream My Data FAQs*, PAC. GAS & ELECTRIC CO., https://www.pge.com/en_US/residential/save-energy-money/analyze-your-usage/your-usage/view-and-share-your-data-with-smartmeter/reading-the-smartmeter/stream-your-data-faq.page [https://perma.cc/X8TG-GJBB] (explaining smart meter integration with smart home devices).

10. Samuel J. Harvey, Note, *Smart Meters, Smarter Regulation: Balancing Privacy and Innovation in the Electric Grid*, 61 UCLA L. REV. 2068, 2079 (2014).

occupied.[11] Solar providers could use this information to tailor their product offerings to match a consumer's energy-consumption level.[12] Researchers have even proposed examining energy-usage patterns to check on the health of elderly people who live alone.[13] This data, in many ways, are a marketer's dream.[14] Would it not be great to be able to tell consumers exactly how much money or energy they would save if they switched to a more efficient water heater?

In both the public and private contexts, then, there is substantial use for this data. It provides unique value to those seeking to better manage the electric grid and design energy-efficiency programs. It allows law enforcement to better understand what is happening inside homes to better solve crimes. And it allows for a whole new approach to targeted marketing of the home and the creation of smart homes. But, in all these cases, consumers are left without a ready means of declining to participate. Many utilities have required the installation of smart meters and, absent extreme measures, it is difficult to forgo access to the electric grid.[15]

---

11. April Weismann, *How Does Occupancy and Vacancy Impact Insurance?*, HPM INS. (Jan. 3, 2018, 11:55 AM), https://www.hpminsurance.com/blog/how-does-occupancy-and-vacancy-impact-insurance [https://perma.cc/VV8F-RPKR].

12. Alexandra B. Klass & Elizabeth J. Wilson, *Remaking Energy: The Critical Role of Energy Consumption Data*, 104 CALIF. L. REV. 1095, 1102 (2016).

13. José Alcalá et al., *Detecting Anomalies in Activities of Daily Living of Elderly Residents via Energy Disaggregation and Cox Processes*, *in* PROCEEDINGS OF THE 2ND ACM INTERNATIONAL CONFERENCE ON EMBEDDED SYSTEMS FOR ENERGY-EFFICIENT BUILT ENVIRONMENTS 225, 225 (2015). Using device disaggregation, researchers believe that they can tell enough about the living patterns of these elderly residents to determine when those patterns have been unduly disrupted by a health event. *Id.* at 233. The critical advantage of such monitoring is that it requires no additional sensors—the smart meter itself is enough. *See* BOSCH SOFTWARE INNOVATIONS GMBH, WHICH NEW SERVICES CAN ENERGY PROVIDERS OFFER IN THE IOT ENVIRONMENT? 14 (2018), https://www.bosch-si.com/connected-energy/insights/downloads/new-businessmodels.html [https://perma.cc/CKQ5-PNBT] (commenting on this possibility, among others).

14. A major advertising agency even "announced that it was teaming up with a London-based software company to study ways to collect smart meter data, saying that it would 'open the door of the home.'" Natasha H. Duarte, Recent Development, *The Home Out of Context: The Post*-Riley *Fourth Amendment and Law Enforcement Collection of Smart Meter Data*, 93 N.C. L. REV. 1140, 1156 (2015). Some companies have already started tracking this kind of data, including smart-television companies such as VIZIO and insurance companies such as Blue Cross Blue Shield, which tracks when consumers utilize sleep-apnea devices. *See* Marshall Allen, *You Snooze, You Lose: How Insurers Dodge the Costs of Popular Sleep Apnea Devices*, NPR (Nov. 21, 2008, 5:00 AM), https://www.npr.org/sections/health-shots/2018/11/21/669751038/you-snooze-you-lose-how-insurers-dodge-the-costs-of-popular-sleep-apnea-devices [https://perma.cc/4AT2-KHZD]; Ben Gilbert, *There's a Simple Reason Your New Smart TV Was So Affordable: It's Collecting and Selling Your Data, and Serving You Ads*, BUS. INSIDER (Apr. 5, 2019, 9:27 AM), https://amp.businessinsider.com/smart-tv-data-collection-advertising-2019-1 [https://perma.cc/7WAJ-9GLD].

15. *See infra* Section II.C.

This lack of consumer choice and the detailed nature of the records lead us to believe that people have an expectation of privacy in energy-usage records and that the government should be required to obtain a warrant if it wishes to access those records for law enforcement purposes. The analysis required to reach this conclusion works differently for public and private utilities. To begin, consider private utilities. Traditionally, the Fourth Amendment did not protect this kind of information when it was held by a private third party; the United States Supreme Court had held that people do not have privacy interests in the information that they voluntarily share with institutions such as banks and telephone companies.[16] Under this logic, energy-usage data in the hands of a private utility would be treated as public information for Fourth Amendment purposes.[17] But the Supreme Court's recent decision in *Carpenter v. United States*[18] has shown a new openness to granting protection in cases, like this one, where the introduction of new technology has fundamentally shifted the nature of the privacy invasion and people do not have a meaningful ability to avoid having their private behavior exposed.[19] Going forward, courts should recognize that consumers' inability to effectively opt out of smart meter usage means they have not voluntarily consented to the sharing of this data.

The Fourth Amendment analysis takes a different form in the public utility context.[20] Here, one must first distinguish between law enforcement and non-law enforcement uses of the data. When the Fourth Amendment is implicated, collection of information for law enforcement purposes generally requires a warrant or an exception to the warrant requirement, but collection of information for non-law enforcement purposes is governed under a more open reasonableness standard.[21] Since public utilities need granular energy-usage data for the purpose of better managing the electric grid, we believe it is reasonable for the government to collect that information for that purpose. It is unreasonable, however, for the government to then repurpose this same information for use by law enforcement absent a warrant given the intrusiveness of the data and the way in which they allow the government to peer into the home. This complex area of doctrine affects the privacy rights of the nearly 15% of Americans who are serviced by a public utility.[22]

---

16. *See infra* Section II.A.

17. *See infra* Section II.A.

18. 138 S. Ct. 2206 (2018).

19. *Id.* at 2223 (protecting cell phone location records despite several dissents).

20. Though Natasha Duarte argued that the third-party doctrine should not apply to smart meter data, Duarte, *supra* note 14, at 1153, this Article is the first to address how the Fourth Amendment should regulate information collection by public utilities.

21. *See Carpenter*, 138 S. Ct. at 2221.

22. *Stats and Facts*, AM. PUB. POWER ASS'N, https://www.publicpower.org/public-power/stats-and-facts [https://perma.cc/5C7F-TX5Y].

The same lack of consumer choice that is important in the Fourth Amendment context should lead Congress and state legislatures to pass new laws protecting energy privacy from both governmental and non-governmental intrusion. Previous work in this area has addressed the challenge of standardizing energy-usage information to allow for greater information sharing, pointing to the many potential benefits of granting private actors access to this wealth of data.[23] We differ from these scholars in believing the extreme usefulness of this data poses a substantial danger to individual privacy.[24] We therefore propose an aggressive regime that gives utilities the broad ability to use this data for grid management but restricts further uses by third parties such as marketers or energy-efficiency companies. Specifically, utilities should only be able to share anonymized consumer data or aggregated data from a specific town or community. If utilities desire to share specific consumer information, they must obtain the consent of the consumer first and this consent must be treated as limited in time and scope. These principles should be codified by administrative regulations and vigorously enforced by agency actions.

Part I of this Article provides background on the changing landscape of energy management in the United States and introduces the fundamental privacy trade-off of smart meters, examining the ways in which they can expose the activities of the home. Part II analyzes the intersection of smart meter data with Fourth Amendment privacy protections. It considers both how the third-party doctrine should apply to smart meters as well as how to think about the Fourth Amendment when the government acts as a utility rather than as an enforcer of criminal law. It also considers the interplay between public and private privacy standards. In Part III, we move beyond the government context and consider the kinds of legal protections necessary to prevent the exploitation of energy-usage data by private parties. To this end, we recommend a federal statute that regulates the sharing of energy-usage data and provides restrictions for which entities can access the data and for what purposes. Finally, this Article concludes by recognizing that smart meters will be necessary for effective grid management in the context of climate change and the increasing need to better manage energy resources. But it cautions against the unregulated development of smart meters and smart homes due to the need to protect the privacy of

23. Klass & Wilson, *supra* note 12, at 1102–03 (noting that the article "focus[ed in part] on the difficulty in obtaining such information and its potential uses if gathered on a large scale").

24. *Id.* at 1157 ("Concerns over reidentification of individual or residential energy consumption data are generally less pressing than in other contexts, such as with health care or education data."); *id.* at 1158 (asserting that "the privacy or confidentiality interests in energy consumption data may be overstated").

people within what is perhaps the last sacred place recognized by Fourth Amendment law—the home.

I. THE CHANGING AMERICAN ELECTRIC GRID

In this Part we begin by considering how smart meters have changed the nature of the American electric grid. The modern electric power system, also known as the grid in the United States, is comprised of generation units, transmission lines, and distribution wires.[25] Electricity is produced at generation units such as coal and natural gas power plants, carried long distances—sometimes across several states—by transmission lines, and then finally delivered to the end users along distribution wires.[26] The demand for electricity can vary considerably hour to hour, day to day, and season to season.[27] Since large-scale storage of electricity is currently difficult, this necessitates the balancing of electricity production and demand.[28] If supply is unable to meet demand, local blackouts or brownouts can result.[29] Though this is unusual in the United States, even here, isolated failures in the transmission or distribution systems can trigger a cascade of breakdowns when demand

25. EISEN ET AL., ENERGY, ECONOMICS, AND THE ENVIRONMENT 66 (4th ed. 2015).

26. *See How Electricity Is Delivered to Consumers*, U.S. ENERGY INFO. ADMIN., https://www.eia.gov/energyexplained/electricity/delivery-to-consumers.php [https://perma.cc/5DYL-544C] (last updated Oct. 11, 2019).

27. *Electricity Demand Changes in Predictable Patterns*, U.S. ENERGY INFO. ADMIN. (Dec. 6, 2011), https://www.eia.gov/todayinenergy/detail.php?id=4190 [https://perma.cc/M6GP-EGM5] ("Changes in electricity demand levels are generally predictable and have daily, weekly, and seasonal patterns.").

28. EISEN ET AL., *supra* note 25, at 67 ("This means that whenever customers turn the power on or off the generating load must be increased or decreased almost instantaneously to avoid affecting the voltage significantly."); NEXIGHT GRP., U.S. DEP'T OF ENERGY, ELECTRIC POWER INDUSTRY NEEDS FOR GRID-SCALE STORAGE APPLICATIONS 5 (2010), https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Utility_12-30-10_FINAL_lowres.pdf [https://perma.cc/DV67-DYCQ]; Felix Barber, *The Future of Energy Storage: A Lost Opportunity for the U.S.?*, HARV. U.: SCI. POL'Y (Dec. 6, 2017), http://sitn.hms.harvard.edu/flash/2017/future-energy-storage-lost-opportunity-u-s/ [https://perma.cc/6JQS-APJK] ("Despite its sparse use at present, energy storage, and in particular batteries, could dramatically change the nature of [the grid] system. This could happen by both offsetting the maximum power supply required from these power plants, and by allowing renewables to provide a larger contribution than is possible with conventional electric grids."); Marshall Brain & Dave Roos, *How Power Grids Work*, HOWSTUFFWORKS (Apr. 1, 2000), https://science.howstuffworks.com/environmental/energy/power.htm [https://perma.cc/7RJH-HNBA].

29. Sara Hoff, *U.S. Electric System Is Made Up of Interconnections and Balancing Authorities*, U.S. ENERGY INFO. ADMIN. (July 20, 2016), https://www.eia.gov/todayinenergy/detail.php?id=27152 [https://perma.cc/W6E2-YKRV].

for electricity is high, for example on the hottest day in summer.[30] This can lead to blackouts for millions of people.[31]

Demand fluctuates over the course of the day, the season, and the year. As demand rises during peak periods—which is commonly in the late afternoon or early evenings when everyone arrives home from work or school[32]—more power plants must come online and provide the additional electricity required for that short period of time.[33] These "peaker" electricity generators are idle much of the time and generally are the least economical sources; the cheapest and most efficient power generators run constantly.[34] This careful balancing of supply and demand of electricity gives rise to one of the recurring obsessions of modern energy management: the shifting of demand from peak periods to off-peak periods to reduce costs.[35]

---

30. In 2003, the United States suffered its largest blackout, which resulted in "50 million people across eight states and two Canadian provinces" losing power in eight minutes. Massoud Amin & Phillip F. Schewe, *Preventing Blackouts: Building a Smarter Power Grid*, SCI. AM. (Aug. 14, 2017), https://www.scientificamerican.com/article/preventing-blackouts-power-grid/ [https://perma.cc/K3PU-B2UJ].

31. Marshall Brain & Julia Layton, *How Blackouts Work*, HOWSTUFFWORKS (Aug. 15, 2003), https://science.howstuffworks.com/environmental/energy/blackout.htm [https://perma.cc/FD4K-45QB] ("In nearly every major blackout, the situation is the same. One piece of the system fails, and then the pieces near it cannot handle the increased load caused by the failure, so they fail. The multiple failures make the problem worse and worse, and a large area ends up in the dark."); *see* Brain & Roos, *supra* note 28.

32. EISEN ET AL., *supra* note 25, at 74; Beia Spiller, *All Electricity Is Not Priced Equally: Time-Variant Pricing 101*, ENVTL. DEF. FUND: ENERGY EXCHANGE (Jan. 27, 2015), http://blogs.edf.org/energyexchange/2015/01/27/all-electricity-is-not-priced-equally-time-variant-pricing-101/ [https://perma.cc/ZQQ6-3G3W].

33. EISEN ET AL., *supra* note 25, at 74; Jeff St. John, *Dueling Charts of the Day: Peaker Plants vs. Green Power*, GREENTECH MEDIA (Jan. 17, 2014), https://www.greentechmedia.com/articles/read/dueling-charts-of-the-day-peaker-plants-vs-green-power [https://perma.cc/7AGM-3H56]; *see* Bethel Afework et al., *Peaking Power*, ENERGY EDUC., https://energyeducation.ca/encyclopedia/Peaking_power [https://perma.cc/87DB-QYPA] (last updated Sept. 3, 2018) ("Natural gas power plants are the most common peaker power plants as they are dispatchable. This means they can be turned on or off and their output can change quite quickly.").

34. EISEN ET AL., *supra* note 25, at 74 ("Generally, the electrical grid is organized so that the least expensive available generation is used to meet the next increment of demand. When demand is modest, the cheapest generators are able to satisfy it, resulting in modest prices. However, during peak periods, all generation resources—even the most expensive—must be called upon."); Mike Orcutt, *How a Smarter Grid Can Prevent Blackouts—and Cut Your Energy Bills*, POPULAR MECHANICS (Aug. 6, 2010), https://www.popularmechanics.com/science/energy/a6013/how-a-smarter-grid-can-prevent-blackouts/ [https://perma.cc/NE4N-5CK5] ("Less than half of the generation capacity in the U.S. comes from power plants designed to run all the time to meet demand. . . . Reserve plants are much more expensive to operate, resulting in large disparities in generation costs throughout the day and year.").

35. Spiller, *supra* note 32 (explaining the use of time-variant pricing to shift demand).

A. *Smart Meters as Energy-Management Tools*

Smart meters are a key tool for monitoring electricity demand throughout the day. Use of electricity by consumers is generally tracked by a meter that is installed on the consumer's home or office.[36] Traditionally, these meters were analog.[37] A meter reader would come in person once per month and, by examining the meter, determine that the meter recorded 900 kilowatt-hours of electricity since it was last read.[38] The utility would then bill the consumers for this monthly household total.[39] Neither the consumer nor the utility knew anything other than the monthly total, however.[40] There was no way to tell exactly *when* the electricity was consumed at the home.[41]

This system for recording energy usage is changing. Smart meters have replaced the traditional analog meters over the past decade, and as of December 2018 almost 70% of residential units in the United States have smart meters installed.[42] Smart meters themselves come in various types.[43] The "dumbest" smart meters merely permit automated meter reading (AMR); they broadcast monthly usage information.[44] One variant of AMR required a van to drive through neighborhoods and send out radio signals to query the AMR meters so they would broadcast their current usage.[45] But more advanced smart meters can be in continuous

---

36. *See* Timothy Thiele, *How an Electric Meter Reads Power Usage*, SPRUCE, https://www.thespruce.com/how-electric-meters-read-power-1152754 [https://perma.cc/ZU9D-5QER] (last updated June 26, 2019).

37. *See id.*

38. *See id.*

39. Brief of Amici Curiae Electronic Frontier Foundation & Privacy International in Support of Plaintiff-Appellant Naperville Smart Meter Awareness & Reversal at 3, 18 n.31, Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521 (7th Cir. 2018) (No. 16-3766).

40. Karl Bode, *Your Smart Electricity Meter Can Easily Spy on You, Court Ruling Warns*, VICE: MOTHERBOARD (Aug. 24, 2018, 9:00 AM), https://www.vice.com/en_us/article/j5n3pb/your-smart-electricity-meter-can-easily-spy-on-you-court-ruling-warns [https://perma.cc/LL5R-JL2F].

41. *Id.*

42. ADAM COOPER & MIKE SHUSTER, THE EDISON FOUND. INST. FOR ELEC. INNOVATION, REPORT: ELECTRIC COMPANY SMART METER DEPLOYMENTS: FOUNDATION FOR A SMART GRID (2019 UPDATE) 1 (Dec. 2019), https://www.edisonfoundation.net/iei/publications/Documents/IEI_Smart%20Meter%20Report_2019_FINAL.pdf [https://perma.cc/UUD6-9J5E].

43. *E.g.*, Tim J. Smith, *Shifting Paradigm: Automated Meter Reading (AMR)*, WIGLAF J. (Sept. 2003), https://www.wiglafjournal.com/industry/energy-utilities/2003/09/shifting-paradigm-automated-meter-reading-amr/# [https://perma.cc/HY4B-7LXW].

44. *Smart vs AMR Meters: What Is the Difference?*, YŪ ENERGY (Feb. 6, 2019), https://www.yuenergy.co.uk/news/smart-vs-amr-meters-what-is-the-difference [https://perma.cc/3B64-34RM].

45. *See* Dan Benelisha Itron, *For Safety's Sake: AMR Technology Helps Take Meter Readers, Customers Out of Harm's Way*, ELECTRIC ENERGY T&D MAG. (May/June 2002), https://

communication with the local utility.[46] These more advanced smart meters are part of a larger push for the development of the "smart grid" and advanced metering infrastructure (AMI).[47] AMI enables two-way communication between customers and their utilities.[48] An AMI-style smart meter can transmit usage information to the utility, receive from the utility various pieces of data (such as current power costs), and even interface with home energy hubs.[49] If traditional analog meters are like classic landline telephones, then AMR meters are equivalent to 1990s-style flip cell phones and 2010s-style AMI smart meters are the iPhone.

When speaking of smart meters, we have in mind these "smarter" smart meters.[50] Once installed on a home, these smart meters automatically and remotely transmit consumer electricity-usage data to utility companies in short intervals, sometimes with several readings per

---

electricenergyonline.com/energy/magazine/36/article/For-Safety-s-Sake-AMR-Technology-Helps-Take-Meter-Readers-Customers-Out-of-Harm-s-Way.htm [https://perma.cc/S6KF-2LJA].

46. *See, e.g.*, *Smart vs AMR Meters: What Is The Difference?*, *supra* note 44 ("AMR meters only provide kWh information and possible peak kW demand for the month. Smart meters send a lot more information, including[:] cumulative kWh usage, daily usage, peak kW demand, voltage information, outage information, time of use kWh and peak kW readings.").

47. *See* ADAM COOPER, THE EDISON FOUND. INST. FOR ELEC. INNOVATION, REPORT: ELECTRIC COMPANY SMART METER DEPLOYMENTS: FOUNDATION FOR A SMART GRID 3 (2017); Raymar Rashed Mohassel et al., *A Survey on Advanced Metering Infrastructure*, 63 ELECTRICAL POWER & ENERGY SYSTEMS 473, 474 (2014)

> AMI is not a single technology; rather, it is a configured infrastructure that integrates a number of technologies to achieve its goals. The infrastructure includes smart meters, communication networks in different levels of the infrastructure hierarchy, Meter Data Management Systems (MDMS), and means to integrate the collected data into software application platforms and interfaces.

The Smart Home, SMARTGRID.GOV, https://www.smartgrid.gov/the_smart_grid/smart_home.html [https://perma.cc /LWN4-VGP3] ("Smart meters provide the Smart Grid interface between you and your energy provider.").

48. *See* Mohassel et al., *supra* note 47, at 475.

49. *See id.*; *see also* U.S. DEP'T OF ENERGY, *supra* note 7, at 10.

> Control technologies include devices such as programmable communicating thermostats (PCTs) and direct load control (DLC) devices that utilities and customers use to automatically control customers' heating and cooling systems or other energy-intensive devices. In addition, home-area networks (HAN) and energy management systems can be installed to automatically control appliances in response to price signals, load conditions, or pre-set preferences. (emphasis omitted).

50. In addition to raising greater privacy challenges, AMI systems are also now more common in the United States. *See* Harvey, *supra* note 10, at 2072; Marc Harnish, *Electricity Monthly Update, Highlights: February 2015*, U.S. ENERGY INFO. ADMIN. (Apr. 27, 2015), https://www.eia.gov/electricity/monthly/update/archive/april2015/ [https://perma.cc/3FG7-VZB7]; COOPER & SHUSTER, *supra* note 42.

hour.[51] This greatly increases the amount of information available to utilities, allowing for a variety of new efficiencies but coming at the expense of consumer privacy.

Smart meters are produced by a variety of manufacturers and have different levels of functionality. Many use Zigbee, a data transmission protocol specifically intended for the conveyance of information by low-power, low-bandwidth radios, including smart meter data.[52] But variations exist, and not all smart meters have the same capacity to interface with consumer products such as smart thermostats, smart appliances, and energy dashboards.[53] And not all utilities have been equally active in incorporating consumers into the power-management process. For example, a utility in Ohio offers an "easy-to-use app" that allows the user to see energy usage over time, determine how much energy is drawn by heating and ventilation systems, and, with the aid of a free "energy bridge," directly control smart devices straight from the app.[54] In contrast, a utility in New York is currently advertising no

---

51. Christine Horne et al., *Privacy, Technology, and Norms: The Case of Smart Meters*, 51 SOC. SCI. RES. 64, 65 (2015).

52. Joe Ballif, *How Smart Energy by the Zigbee Alliance Enables Service Providers and Consumers to Improve Consumption Habits and Save Money*, ZIGBEE ALLIANCE (June 26, 2018), https://zigbee.org/zigbee-alliance-smart-energy-saving-mony-1/ [https://perma.cc/B38X-Q8LR]; Benjamin Garcia, *ZigBee Smart Energy*, TELDAT (Nov. 6, 2018), https://www.teldat.com/blog/en/zigbee-smart-energy-smart-metering-home-automation/ [https://perma.cc/6NZ4-RQLX].

53. Not even all devices that use Zigbee are able to communicate with each other due to different, and sometimes proprietary, profiles or protocols. *See, e.g.*, J.D. Roberts, *FAQ: Zigbee Application Profiles, or Why Not All Zigbee Devices Work with SmartThings*, SMARTTHINGS COMMUNITY (June 25, 2019, 8:28 AM), https://community.smartthings.com/t/faq-zigbee-application-profiles-or-why-not-all-zigbee-devices-work-with-smartthings/76219 [https://perma.cc/T498-QRVP]. This concern seems to have been mitigated with the release of Zigbee 3.0. *See, e.g.*, Mike Bleakmore, *Understanding the Zigbee 3.0 Protocol*, DIGI (Apr. 19, 2018), https://www.digi.com/blog/understanding-the-zigbee-3-0-protocol/ [https://perma.cc/HYY8-PHT2]. Products are therefore sometimes advertised as being compatible with specific utility providers. *See, e.g.*, *Supported California Utilities*, RAINFOREST AUTOMATION, https://rainforestautomation.com/state-california-residents/ [https://perma.cc/PPF4-KP4W]. For example, at least some utilities in six states (California, Texas, Illinois, Vermont, Hawaii, and Pennsylvania) support the Rainforest Eagle 200 Energy Monitoring Gateway. *Supported Utilities*, RAINFOREST AUTOMATION, https://rainforestautomation.com/utilities/ [https://perma.cc/XTP2-GCR7]. This device uses Zigbee to communicate directly with a compatible smart meter and display real-time energy-consumption information. *See EAGLE-200™ Intelligent Control Gateway*, RAINFOREST AUTOMATION (2017), https://rainforestautomation.com/wp-content/uploads/2017/10/eagle-200-datasheet_1.3.pdf [https://perma.cc/NYT5-9YH8].

54. *Smart Meter Technologies*, AEP OHIO, https://www.aepohio.com/info/smartmeters/technologies.aspx [https://perma.cc/ZY49-WX2T]; *Enhance your App Experience*, AEP OHIO, https://itsyourpowerohio.com/energy-bridge/ [https://perma.cc/9JM8-QS8L]. The utility DTE Energy, based in Detroit, uses a similar program that connects an app with an Energy Bridge to enable customs to connect their smart home devices and therefore better control their energy usage. *DTE Insight FAQs*, DTE ENERGY, https://newlook.dteenergy.com/wps/wcm/connect/dte-web/insight/dte-insight-faq [https://perma.cc/8YHG-NPTL].

consumer-facing analytics and no compatibility with third-party products.[55] Perhaps due to differences across utilities,[56] some home energy-monitoring products opt for more direct approaches to measurement. One product uses the infrared port found on most smart meters to avoid any radio-connectivity issues.[57] Another requires an electrician to install clamps on the power mains, bypassing the meter entirely.[58]

Despite some variability in consumer friendliness, smart meters are extremely helpful for utilities. Take the basic issue of service outages. Prior to the installation of smart meters, utilities only knew where an outage occurred in their service territory when a customer called to report it[59]—remember that the meters themselves had no means of reporting back to the utility. But the smart grid allows utilities to directly detect when and where outages are occurring, which also gives them a head start

55. *See* Mark Harrington, *Amid a Sea of Smart Meters, New Time-of-Use Rates Also Are Coming*, NEWSDAY, https://www.newsday.com/long-island/pseg-smart-meters-rates-1.30602551 [https://perma.cc/B55V-S7WV] (last updated May 5, 2019, 11:08 PM) (describing the introduction of time-of-use rates by PSEG Long Island); *Dispelling the Myths and Misconceptions of Smart Meters*, PSEG LONG ISLAND, https://www.psegliny.com/myaccount/serviceandrates/smartmeter/faq [https://perma.cc/2625-PBN8] (promising that the utility will not even view individual-level data). A recent report by ACEEE indicates that most utilities with smart meters installed provide AMI data to customers via a website and mobile device app. AM. COUNCIL FOR AN ENERGY-EFFICIENT ECON., LEVERAGING ADVANCED METERING INFRASTRUCTURE TO SAVE ENERGY 12 (Jan. 27, 2020), https://www.aceee.org/sites/default/files/publications/researchreports/u2001.pdf [https://perma.cc/93DQ-M6VX].

56. Apparently, utilities have often created unintentional technological barriers to information sharing. *See, e.g.*, Jeff St. John, *Texas Takes a Big Step in Improving Access to Smart Meter Data*, GREENTECH MEDIA (Feb. 6, 2018), https://www.greentechmedia.com/articles/read/texas-smart-meter-data-access#gs.atx1d3 [https://perma.cc/ADD8-GJ8D].

57. This product is Energy Cloud by Blue Line Innovations. *See Easy Do-It-Yourself Installation*, BLUE LINE INNOVATIONS, https://www.bluelineinnovations.com/diy-details [https://perma.cc/F5RW-L8MS] (stating that the meter sensor slides over the meter and uses the customer's home network to transmit data). It claims to be compatible with the vast majority of smart meter types, but no statistics are available. *See Compatible Meters*, BLUE LINE INNOVATIONS, https://www.bluelineinnovations.com/compatibility-window [https://perma.cc/FB78-GFNT].

58. *How It Works.*, SENSE, https://sense.com/product-page [https://perma.cc/2HEF-SAZW]. Efficiency Vermont has partnered with the company, Sense, to help homeowners save energy by identifying individual device energy usage within the home. *Efficiency Vermont and Sense Conduct Pilot Study of Advanced Home Energy Monitoring*, EFFICIENCY VERMONT (July 24, 2018), https://www.efficiencyvermont.com/news-blog/news/efficiency-vermont-and-sense-conduct-pilot-study-of-advanced-home-energy-monitoring [https://perma.cc/AWG9-XTK7].

59. *Smart Meters Can Reduce Power Outages and Restoration Time*, NAT'L ELEC. MFRS. ASS'N, https://www.nema.org/Storm-Disaster-Recovery/Smart-Grid-Solutions/Pages/Smart-Meters-Can-Reduce-Power-Outages-and-Restoration-Time.aspx [https://perma.cc/8NSZ-4PMZ].

in diagnosing *why* the outage is occurring.[60] AMIs provide "situational awareness" to utilities in this way, enabling them to send crews to the highest priority areas during outages and understand what percentage of their service territory is without power.[61] Smart meters also provide utilities with the ability to remotely switch the power supply on or off, which is critical during storms and other natural disasters.[62]

The detailed data provided by smart meters gives utilities almost real-time information on electricity demand, which can enable the utility to better generate the appropriate amount of electricity to meet consumer demand for a specific time of day.[63] This allows for better calibration of production and minimizes surplus electricity.[64] Smart meters can also provide residential and business users real-time information about electricity cost to, hopefully, encourage them to change their

---

60. *See* EXEC. OFFICE OF THE PRESIDENT, ECONOMIC BENEFITS OF INCREASING ELECTRIC GRID RESILIENCE TO WEATHER OUTAGES 10–11 (2013) (describing how the smart grid reduced power-outage duration in the wake of Superstorm Sandy and Hurricane Irene); *How The Smart Grid Keeps Your Power On*, SMART ENERGY CONSUMER COLLABORATIVE, http://www.whatissmartgrid.org/smart-grid-101/fact-sheets/how-the-smart-grid-keeps-your-power-on [https://perma.cc/UGL7-REXE]; *Smart Meters Can Reduce Power Outages and Restoration Time*, *supra* note 59.

61. Jouni Peppanen et al., *Leveraging AMI Data for Distribution System Model Calibration and Situational Awareness*, 6 IEEE TRANSACTIONS ON SMART GRID 2050, 2056 (2015).

> Situational awareness can provide tangible and monetary improvements through increased reliability. Advanced systems provide immediate alerts and early-warning detection of issues. Locations of outages along with potential feeder reconfigurations can be directly known so that crews can be dispatched as efficiently as possible. Situational awareness also provides visualization and detection of problem areas, such as overloaded lines or inefficient buildings.

See also COOPER, *supra* 47, at 3 (describing how smart meter technology allows providers to restore power quickly and efficiently).

62. EISEN ET AL., *supra* note 25, at 900; Kim Zetter, *Security Pros Question Deployment of Smart Meters*, WIRED (Mar. 4, 2010, 6:07 PM), https://www.wired.com/2010/03/smart-grids-done-smartly/ [https://perma.cc/E375-MNR8] ("Digital smart meters have an electronic disconnect switch that allows the utility company to shut down electricity remotely.").

63. *See* Brendan Cook et al., *The Smart Meter and a Smarter Consumer: Quantifying the Benefits of Smart Meter Implementation in the United States*, CHEMISTRY CENT. J., Apr. 2012, at 1, 5 ("A primary goal of smart meter implementation is to better know the demand of every consumer, in order to adapt the supply of electricity. The introduction of various informatics devices has made this possible."); *The Smart Home*, *supra* note 47 ("The Smart Grid, with its System of controls and smart meters, will help to effectively connect all these mini-power generating systems to the grid, to provide data about their operation to utilities and owners, and to know what surplus energy is feeding back into the grid versus being used on site.").

64. *See* Harvey, *supra* note 10, at 2073–74 ("Enhanced monitoring of the location and timing of electricity needs will also mean utilities will be able to better reduce line loss—energy lost in transmission or distribution—and avoid the need for excess generation to ensure demand is met."); Megan McLean, Note, *How Smart is Too Smart?: How Privacy Concerns Threaten Modern Energy Infrastructure*, 18 VAND. J. ENT. & TECH. L. 879, 884 (2016).

consumption patterns.[65] The goal is for consumers to shift some of the electricity usage to earlier or later times in the day to reduce the need to bring more power plants online at peak usage, reducing the cost of providing the power.[66]

For those consumers who wish to understand their energy usage, there are two basic approaches. First, many utilities enable their customers to view their energy usage on the utility website.[67] The clarity and detail of these utility-provided portals tend to vary greatly.[68] Second, third-party companies are starting to develop platforms for consumers to see and manage their electricity usage at home through in-home displays and home energy-management systems.[69] These home systems allow consumers to manage their energy consumption independently and understand whether peak demand is occurring at any given time.[70]

The idea of having individual consumers shift their behavior in response to minute-by-minute changes in electricity pricing sounds somewhat fanciful; few consumers are likely to pay this much attention to their electricity-consumption decisions.[71] But this is where smart

65. EISEN ET AL., *supra* note 25, at 901 ("A smart meter could also show the real-time price of electricity, and help consumers save money. Demand for electricity peaks at various times during the typical day. Using a smart meter, a consumer could time shift and lower her electricity usage when demand and prices are high."); C. Aswin Raj et al., *Smart Meter Based on Real Time Pricing*, 21 PROCEDIA TECH. 120, 120, 124 (2015).

66. Luis I. Minchala-Avila et al., *Design and Implementation of a Smart Meter with Demand Response Capabilities*, 103 ENERGY PROCEDIA 195, 195 (2016) ("Peak load reduction through an interactive reaction of the loads installed at the customer premises, *e.g.* turn on schedulable loads when cheap generation is available, increases network reliability and produce significant economic savings to the utility and the customers.").

67. U.S. ENERGY INFO. ADMIN., AN ASSESSMENT OF INTERVAL DATA AND THEIR POTENTIAL APPLICATION TO RESIDENTIAL ELECTRICITY END-USE MODELING 7 (2015) (describing the Green Button Initiative).

68. *See id.* at 22.

69. Cheryl Dancey Balough, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161, 166–67 (2011). One example of this product is the Energy Cloud by Blue Line Innovations. It reads a smart meter via the meter's infrared port. *See Easy Do-It-Yourself Installation*, *supra* note 57. It claims to be compatible with the vast majority of smart meter types, but no statistics are available. *See Compatible Meters*, *supra* note 57. Commonwealth Edison (ComEd), the utility serving the Chicago metro area provides a customer guide for linking in-home displays to the ComEd smart meter. *See Smart Meter Connected Devices Service: Customer Guide*, COMED, https://www.comed.com/SiteCollectionDocuments/SmartEnergy/SMCD_CustomerGuide.pdf [https://perma.cc/5TYU-Y5QW]. The service allows customers "to receive energy usage and estimated cost information from ComEd through a smart device that is wirelessly connected with the smart meter" on the home. *Id.*

70. A.F.A. Aziz et al., *Artificial Intelligent Meter Development Based on Advanced Metering Infrastructure Technology*, 27 RENEWABLE & SUSTAINABLE ENERGY REVS. 191, 195 (2013).

71. *See* Chris Mooney, *Why 50 Million Smart Meters Still Haven't Fixed America's Energy Habits*, WASH. POST (Jan. 29, 2015, 1:45 PM), https://www.washingtonpost.com/news/energy-

homes and smart devices can play a critical role. What if your thermostat knew it was cheaper to cool down your home in the morning as opposed to the afternoon, when it is hotter and more air-conditioning units are running?[72] Or what if your dishwasher knew it would be cheaper to run now as opposed to in an hour?[73] Much power is consumed by these kinds of consumer appliances, and even now product manufacturers are trying to integrate them with smart home hubs and smart meters.[74] Smart home hubs and smart appliances can respond to signals from utilities.[75] In fact, "[t]here is an extensive interest on remote monitoring of [smart meters] to increase the grid management and metering security."[76] Even if no consumers ever look at their smart meter data, their homes could learn to take advantage of the information provided by the meters to save the homeowners money and the grid electricity.

---

environment/wp/2015/01/29/americans-are-this-close-to-finally-understanding-their-electricity-bills/ [https://perma.cc/8QS2-SEUA] (describing how a lack of transparency inhibits behavioral change). *But see* Mikko Tuomisto, *Non-Intrusive Appliance Load Monitoring (NIALM) System with the Possibility for Users to Follow the Consumption of Individual Electricity Appliances from the Calendar*, 5 INT'L J. ENERGY & POWER ENGINEERING 129, 130–31 (2016) (describing a tool that would allow consumers to help identify unique device activity to better track electricity consumption in their homes).

72. *See, e.g.*, Ashley Carman, *Nest's Thermostat Will Now Adjust Itself Based on Time-of-Use Rates*, VERGE (June 21, 2016, 11:00 AM), https://www.theverge.com/circuitbreaker/2016/6/21/11987378/nest-thermostat-update-time-of-savings-save-money [https://perma.cc/K5EB-VFCD] ("Now the company is launching a 'Time of Savings' feature that claims to save homeowners money by adjusting their house's temperature based on time-of-use rate plans."); *see also Thermostat Incentive*, COMED, https://www.comed.com/WaysToSave/ForYourHome/Pages/ThermostatIncentive.aspx [https://perma.cc/LFR3-TW9K] (describing a program based on automatic time-use adjustment).

73. U.S. DEP'T OF ENERGY, *supra* note 7, at 15–16 (describing how smart devices can allow for remote control of energy-intensive cycles); *The Smart Home*, *supra* note 47 ("Smart appliances will also be able to respond to signals from your energy provider to avoid using energy during times of peak demand.").

74. PETER BRONSKI ET AL., ROCKY MOUNTAIN INST., THE ECONOMICS OF DEMAND FLEXIBILITY: HOW "FLEXIWATTS" CREATE QUANTIFIABLE VALUE FOR CUSTOMERS AND THE GRID 5 (2015), https://rmi.org/insight/the-economics-of-demand-flexibility-how-flexiwatts-create-quantifiable-value-for-customers-and-the-grid/ [https://perma.cc/YY7B-ZSWS] (pointing out that time shifting on uses such as air conditioning, water heating, and electric-vehicle charging could meaningfully lower peak usage without harming domestic-device productivity).

75. Minchala-Avila et al., *supra* note 66, at 196 ("[Smart meters] integrate the ability to remotely manage loads at the end-user premises by monitoring and controlling the customer's devices and appliances."); *The Smart Home*, *supra* note 47 (describing how an energy management system can be programmed to help limit use during peak periods).

76. Yasin Kabalci, *A Survey on Smart Metering and Smart Grid Communication*, 57 RENEWABLE & SUSTAINABLE ENERGY REVS. 302, 308 (2016).

To encourage use of these automatic-management features, many utilities currently offer "demand response" programs,[77] which enable consumers to play a role in balancing the electric grid "by reducing or shifting their electricity usage" to different times of the day.[78] Some programs utilize pricing information to incentivize their customers to shift their energy usage themselves, others utilize "direct load control programs," which allow the utility to remotely cycle air conditioners, thermostats, or water heaters on and off during peak periods of demand.[79] The majority of existing programs require active customer participation, but in the future utilities will be able to assist consumers in shifting their energy usage by utilizing "intelligent load management schemes" that automatically disconnect loads from power when it is "necessary or convenient."[80] These "[o]ptimal scheduling strategies" will enable utilities using home energy management systems to turn on or off home appliances including air-conditioning units, water heaters, washing machines and dryers, microwaves, computers, and more.[81] While most appliances in homes today are not yet capable of being remotely controlled, utilities and manufacturers are working to make appliances "smart" and able to participate in demand response initiatives.[82]

---

77. FED. ENERGY REG. COMM'N, ASSESSMENT OF DEMAND RESPONSE & ADVANCED METERING 21 (2011) (defining "demand response" as "[c]hanges in electric use by demand-side resources from their normal consumption patterns in response to changes in the price of electricity, or to incentive payments designed to induce lower electricity use at times of high wholesale market prices or when system reliability is jeopardized").

78. *Demand Response*, OFF. ELECTRICITY, https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid/demand-response [https://perma.cc/VXB7-EAGW].

79. U.S. DEP'T OF ENERGY, *supra* note 7, at 15 ("Customers received incentives for allowing utilities to use DLC devices to control various types of appliances and equipment—such as air conditioners, water heaters, and swimming pool and irrigation pumps—to reduce peak demands."); *Demand Response*, *supra* note 78; Herman K. Trabish, *The New Demand Response and the Future of the Power Sector*, UTIL. DIVE (Dec. 11, 2017), https://www.utilitydive.com/news/the-new-demand-response-and-the-future-of-the-power-sector/512134/ [https://perma.cc/9W9V-CWVW].

80. Sean Barker et al., *SmartCap: Flattening Peak Electricity Demand in Smart Homes*, 2012 IEEE INT'L CONF. ON PERVASIVE COMPUTING & COMM. 67, 67; *see also* Trabish, *supra* note 79 ("Nearly everything has a chip in it now . . . . If it is controllable, it can help support the grid." (quoting Carly Sorrentino, Spokesperson, Advanced Microgrid Sys.)).

81. Hussain Shareef et al., *Review on Home Energy Management System Considering Demand Responses, Smart Technologies, and Intelligent Controllers*, 6 IEEE ACCESS 24,498, 24,503–04 (2018), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8352822 [https://perma.cc/5AL2-4JM5].

82. Barker et al., *supra* note 80, at 68; *see* Keith Barry, *Whirlpool's New Connected Appliances Simplify the Smart Grid*, REVIEWED, https://www.reviewed.com/laundry/features/whirlpools-new-connected-appliances-simplify-the-smart-grid [https://perma.cc/7XYY-QTSD] (last updated Sept. 12, 2015) ("Appliances equipped with Whirlpool's 6th Sense Live can automatically run when power is cheapest.").

Finally, smart meters enable the increased use of renewable-energy and storage technologies on the grid. Historically, the conventional grid was unidirectional: electricity moved from the power plants outward through the transmission and distribution system to industrial sites, commercial businesses, and residential homes.[83] This arrangement of the electric grid was effective until the development of distributed energy resources (DERs),[84] which include renewable sources of power such as solar panels or wind turbines that are installed at the customer site instead of the utility plant. The placement of DERs at the "end" of the traditional electric grid required the development of a system that could move electricity "bi-directionally," enabling the DERs to move electricity onto the grid instead of simply receiving it from the grid.[85] Moreover, the interval-level data that smart meters provide also enables the integration of DERs onto the grid and may help utilities better "predict the behavior of customer-sited energy resources so that these resources can be utilized more efficiently."[86] In the future, smart meters could help utilities decide whether to bring online a new power plant or instead utilize battery storage or other DERs located at consumer sites to meet increasing electricity demands.[87]

Smart meters already bring clear benefits for both utilities and the public, and they represent a promising area for consumer participation and increased efficiency in the future. Overall, the savings that follow from a better understanding of electricity demand and the potential for peak load shifting "can significantly reduce national energy use and curb energy emissions while addressing pressing geopolitical and

---

83. Kabalci, *supra* note 76, at 304.

84. *See* MIT ENERGY INITIATIVE, UTILITY OF THE FUTURE 2 (2016) ("DERs include demand response, generation, energy storage, and energy control devices, if they are located and function at the distribution level.").

85. Kabalci, *supra* note 76, at 309 ("One of the most important achievements in smart grid is AMI system that is used to measure, acquire, and analyze the data about energy consumption and power quality of each consumer. . . . The bidirectional communication is performed between utility supplier and consumer to improve maintenance, demand management, and planning capability of supplier.").

86. COOPER, *supra* 47, at 5. Oracle has partnered with EnergyHub to create a product that will help utilities connect with and potentially control DERs in customer homes in their service territories. "EnergyHub's platform gives utilities deep insight and control of these edge-of-grid assets, allowing the utility to understand where a DER is located on the grid, forecasting the behavior of that DER, and allowing the utility to manage these devices to provide grid services." Stephen Hill, *Opower and EnergyHub Form a Smart Partnership*, OPOWER BLOG SERIES (Oct. 22, 2019), https://blogs.oracle.com/utilities/opower-and-energyhub-form-a-smart-partnership-v3 [https://perma.cc/CN75-V7TZ].

87. U.S. DEP'T OF ENERGY, *supra* note 7, at 52 ("Looking to the future, AMI can contribute to advanced concepts like vehicle-to-grid applications where utilities can have access to EV storage capacity for meeting system needs.").

environmental concerns related to energy security and sustainability."[88] But there are also risks associated with this information revolution. Smart meters generate significant amounts of data on what is occurring within residential homes, which have privacy implications as technology continues to progress in this area.

B. *Risks Posed by Interval-Level Smart Meter Data*

Smart meters record interval-level data on residential electricity usage, transmit the usage to the utility, and can receive communications from the smart grid including "real-time energy prices [and] remote commands" from the utility.[89] They can record electricity-usage data at an extremely precise level, with different systems using hourly, fifteen-minute, and five-minute increments.[90] "Because of its time granularity, smart meter data shows not only *how much* electricity is being used within a home but also at *what time*."[91] Prior to the installation of a smart meter, residential consumers were receiving a single total amount representing their electricity usage over the length of a month.[92] Now, consumers' energy usage is tracked in thousands of data points per month.[93] From this highly detailed data, one can even potentially determine which individual appliances and devices are being used at any given time within a consumer's home.[94] Previously, energy-consumption records were not all that useful to others or dangerous to privacy. Now that has changed.

By looking at smart meter data in short intervals of time, it is possible to identify which individual appliances are being used at any given time

88. Horne et al., *supra* note 51, at 65.

89. BRANDON J. MURRILL ET AL., CONG. RESEARCH SERV., R42338, SMART METER DATA: PRIVACY AND CYBERSECURITY 1 (2012).

90. Klass & Wilson, *supra* note 12, at 1105 ("Utilities can collect data subhourly (e.g., five-, fifteen-, or thirty-minute intervals), hourly, daily, or monthly and choose whether or not to share it, with whom to share it, and in what format to make it available.").

91. Brief of Amici Curiae Electronic Frontier Foundation & Privacy International in Support of Plaintiff-Appellant Naperville Smart Meter Awareness & Reversal, *supra* note 39, at 6–7 ("Thus, smart meter data is both qualitatively and quantitatively different from analog meter data—shifting from 'one data point reflecting *average* monthly use' to between 750 and 8,640 'distinct and time-stamped data points per month that reflect *actual* energy use' at any given time.").

92. *See supra* notes 37–39.

93. *Supra* note 51 and accompanying text.

94. MURRILL ET AL., *supra* note 89, at 1–2; Kabalci, *supra* note 76, at 309 ("One of the most important achievements in smart grid is AMI system that is used to measure, acquire, and analyze the data about energy consumption and power quality of each consumer."); Eoghan McKenna et al., *Smart Meter Data: Balancing Consumer Privacy Concerns with Legitimate Applications*, 41 ENERGY POL'Y 807, 808 (2012) ("The ability to detect specific activities, however, depends on the time resolution of the consumption data.").

because each appliance "generates a unique electric load 'signature.'"[95] The load signatures of appliances are recorded by smart meters and a consumer's energy usage over time can allow for analysis of daily load profiles "due to spikes corresponding to the switching on and off [of] electrical appliances such as a cooker, kettle, iron, microwave, washing machine[,] etc."[96] This kind of individual appliance information can reveal consumers' "daily schedules (including times when they are at or away from home or asleep), whether their homes are equipped with alarm systems, whether they own expensive electronic equipment such as plasma TVs, and whether they use certain types of medical equipment."[97] Moreover, more appliance manufacturers are starting to make smart appliances—those that are able to connect to and communicate with smart meters.[98] Currently, this represents only a moderate threat to privacy because though overall energy-usage data already reveals much, disaggregation of the data to reveal everything is still difficult. In the future though, there will be an even greater threat because smart network integration will make it much easier to disaggregate individual appliances from the overall load.

95. MURRILL ET AL., *supra* note 89, at 4.

96. GRZEGORZ DUDEK ET AL., ANALYSIS OF SMART METER DATA FOR ELECTRICITY CONSUMERS (2018) ("Load density profiles inform about the distribution of the customer load in a given time period. They can be used for comparison the variability of the consumer in different period of the year or in different days of the week. We can also compare different customers using their density profiles.").

97. MURRILL ET AL., *supra* note 89, at 4 (quoting U.S. DEP'T OF ENERGY, DATA ACCESS AND PRIVACY ISSUES RELATED TO SMART GRID TECHNOLOGIES 2 (2010)).

98. Balough, *supra* note 69, at 166 ("The appliances continually send their energy usage, labeled as consumed by that appliance, to the smart meter. The smart meter reads that communication from all smart appliances and can generate a load signature for each home.").

Figure 1: A Household's Power Demand as Measured with Smart Meter Data[99]

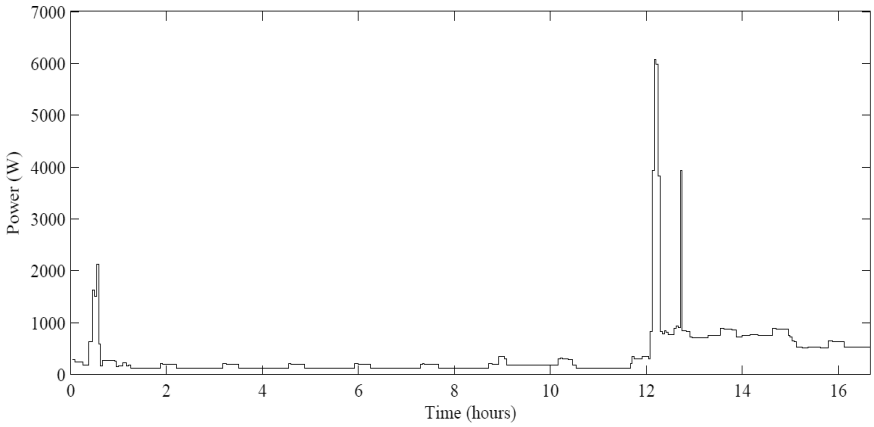
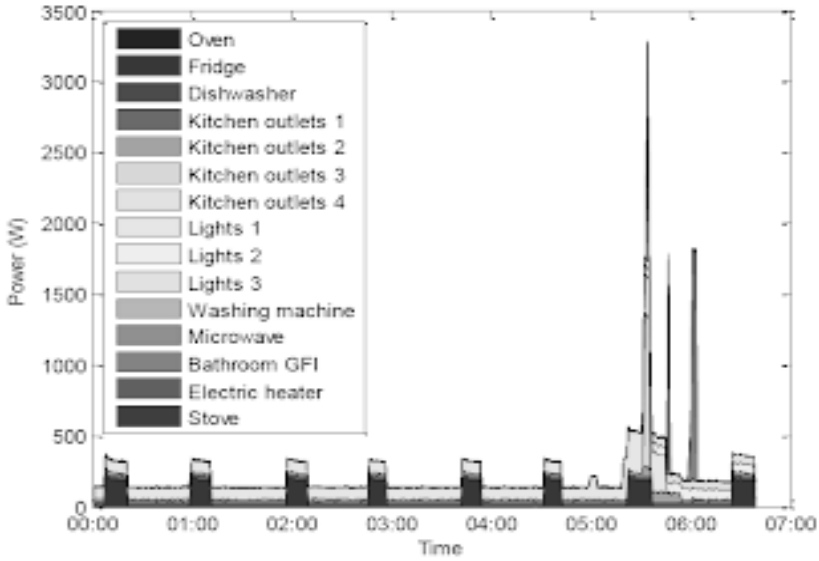


Figure 2: A Household's Power Demand Disaggregated into Appliances[100]



99. Oliver Parson, Unsupervised Training Methods for Non-Intrusive Appliance Load Monitoring from Smart Meter Data 63 fig.6.1(a) (Apr. 2014) (unpublished Ph.D. thesis, University of Southampton), https://eprints.soton.ac.uk/364263/1/Parson-thesis.pdf [https://perma.cc/35P3-NVVY].

100. Oliver Parson, *PhD Work*, http://www.oliverparson.co.uk/phd-work [https://perma.cc/R4V9-LMY5] (last updated Jan. 9, 2014, 6:53 AM). This Figure was generated using hidden Markov modeling to identify individual devices from nonintrusive load monitoring. See Parson et al., *supra* note 8, at 4, for more information on this process.

The interconnectedness of smart meters and smart devices creates an opportunity for increased insight and efficiency.[101] In addition to appliance manufacturers working to develop smart appliances that will interface with smart meters, other companies such as Google, General Electric, and Cisco are also working to create products that will help consumers better analyze their smart meter data and energy consumption.[102] All of these developments are occurring concurrently with the development of smart speakers, smart digital assistants, and other smart devices in the home that can be connected to or integrated with the home energy management system.[103] Google, Apple, and Amazon are also partnering with other companies to link their voice-operated products with the smart-appliance ecosystems, which currently includes home assistants, smart TVs, smart speakers, smart lights, and smart thermostats.[104] As it stands, "[a]bout 60% of Amazon Echo and Google Home users have at least one household accessory, such as a thermostat, security system, or appliance, connected to them,"[105] and these companies are working to achieve ever-greater levels of integration across their smart device product lines.[106] Linking all of this consumer

101. Shareef et al., *supra* note 81, at 24,501.

> Several enabling smart technologies result in the integration of intelligent [home energy management systems] with various functions inside homes, such as automatic control, connection to the utility by a smart meter, and minimized energy consumption. With smart technologies, customers can control household appliances, optimize electricity consumption, and set a schedule for household appliances during critical peak hours based on the DR signals. (footnote omitted).

See supra note 54 (describing an Ohio utility's app that leverages interconnectivity for energy management and a similar Detroit program). The companies Bidgely and EnergyHub are partnering to disaggregate home energy data for more than fifteen home energy device brands. This will allow them to provide customized household and appliance-level data for each home. Julian Spector, *Bidgely and EnergyHub Team Up to Combine Home Energy Data with Controls*, GREENTECH MEDIA (Jan. 30, 2019), https://www.greentechmedia.com/articles/read/bidgely-and-energyhub-team-up-to-combine-home-energy-data-with-controls [https://perma.cc/T79Q-Z8ER].

102. Harvey, *supra* note 10, at 2074.

103. *See* Allegra Bianchini, Note, *Always On, Always Listening: Navigating Fourth Amendment Rights in a Smart Home*, 86 GEO. WASH. L. REV. ARGUENDO 1, 6–7 (2018) ("Integration to control lightbulbs, smart meters, and phone apps, like Uber, allows nearly complete virtual control of a user's home, and the possibility of more capabilities is limited only by programmers' imaginations." (footnote omitted)).

104. Brian Dumaine, *It Might Get Loud: Inside Silicon Valley's Battle to Own Voice Tech*, FORTUNE (Oct. 24, 2018), http://fortune.com/longform/amazon-google-apple-voice-recognition/ [https://perma.cc/28KW-NXZK].

105. *Id.*

106. Apple, Amazon, and Google are partnering to create a single standard for smart-home products. This will enable more connections between smart devices such as lights, thermostats,

data to the smart meter installed in the home would basically invite these companies to sit in your home and to watch, listen, and record everything that you do. And as more utilities partner with tech companies to facilitate the connection between these devices, the higher the risk that consumer energy-consumption data will be easily accessed and sold.

Though this fully "smart home" may be far off in the future, these tech companies are already looking for ways to expand their internet-connected devices to attain information on consumers' personal energy use in the home.[107] Google already has partnerships with utilities and power providers in Illinois, California, and Texas, while Amazon has partnered with EDF Energy in the United Kingdom and Arcadia Power in the United States to provide a bundle of home devices that enable better energy management.[108] The movement of tech companies in the consumer-energy space represents an area of heightened privacy risks.

As of today, utilities are the primary recipient of smart meter data, but the amount and kind of information now collected will be useful to many other parties.[109] Moreover, with the continued development of the smart grid and greater emphasis on energy-efficiency programs at the customer level, utilities will likely struggle to decide which third-party vendors should have access to the smart meter data.[110] Third-party vendors are already seeking access to this data to help them identify potential customers, learn which products are used most in a home, and market

---

and other electronic devices in the home. Ben Gilbert, *In a Rare Move, Apple, Amazon, and Google Just Announced a Major Partnership*, BUS. INSIDER (Dec. 18, 2019), https://www.businessinsider.com/apple-amazon-google-partner-on-smart-home-tech-2019-12 [https://perma.cc/CR7A-YD2X].

107. *See* Bradley Olson, *Google, Amazon Seek Foothold in Electricity as Home Automation Grows*, WALL ST. J. (Jan. 27, 2019, 6:44 PM), https://www.wsj.com/amp/articles/google-amazon-seek-foothold-in-electricity-as-home-automation-grows-11548604800 [https://perma.cc/G3WJ-PJFR].

108. *Id.*; *see EDF Energy Launches Voice Controlled Energy Accounts with Amazon Alexa*, EE ONLINE (Sept. 15, 2016), https://electricenergyonline.com/article/organization/28120/596851/EDF-Energy-launches-voice-controlled-energy-accounts-with-Amazon-Alexa.htm [https://perma.cc/VB4Z-BLX6] ("EDF Energy's collaboration with Amazon is part of the company's commitment to making energy easy and putting customers in control through connected home technologies and other innovative products and services, such as its smart thermostat HeatSmart, and the Show Me Your Bill functionality in its app.").

109. John R. Forbush, Comment, *Regulating the Use and Sharing of Energy Consumption Data: Assessing California's SB 1476 Smart Meter Privacy Statute*, 75 ALB. L. REV. 341, 342 (2012) ("The potential for utilities and other vendors to collect and aggregate energy consumption data from individual homes and businesses raises significant questions about the access, use, and ownership of energy consumption information.").

110. Balough, *supra* note 69, at 169 ("Companies that manufacturer [sic] home [energy management systems] and in-home display systems are actively marketing their products to utilities for distribution to the electric company's residential customers.").

their products to targeted groups of people.[111] These companies could also help develop interfaces for consumers to better understand and manage their energy consumption. "Because myriad other systems that will interact with smart meters have yet to be designed, one cannot fully predict the types and amounts of personally identifiable information that will be monitored or collected."[112]

Law enforcement agencies will also be interested in accessing this data and there is at least one case where a police department accessed smart meter data following a murder.[113] In future cases, electricity-consumption data can be expected to be even more indicative of activities occurring in the home. The problem facing consumers now is "[i]nformation that previously required surveillance and constant monitoring, such as when users are home, their day-to-day schedules, which room of the house they are in at what time, and how often they use certain appliances and security, [will] now [be] conveniently logged into a record."[114] Both third-party companies and law enforcement agencies will be particularly motivated to access that record to attain more information about the consumers and their homes.

As this Part has demonstrated, smart grid developments can help consumers reduce their energy consumption and make the electric grid more efficient. But smart meters, working in conjunction with smart appliances and other smart devices in the home, convey a significant amount of private consumer data to utilities and potentially to their energy efficiency partners. Instead of gathering one data point on energy consumption per month, utilities are now gathering thousands of data points from a consumer's home, which can expose a wide variety of otherwise private activities.

II. PRIVACY PROTECTIONS AND THE EVOLVING MODERN HOME

This Part uses the lens of Fourth Amendment law to analyze the privacy implications of the smart meter revolution. It begins by analyzing the challenges of extending privacy protection to information that is necessarily shared with third parties and the role of the home as a constitutional trump card in the Fourth Amendment analysis. It then applies the traditional Fourth Amendment tests to the problem of smart

111. *See* Harvey, *supra* note 10, at 2079 ("Third-party researchers and companies are seeking access to this data in order to identify customers, enhance product design, and conduct more in-depth analysis of energy consumption. For example, a company could use AMI data to identify potential customers that could benefit from energy efficiency upgrades. That company could then market products and services tailored specifically for those individual customers." (footnote omitted)).

112. Balough, *supra* note 69, at 167.

113. *See supra* note 3 and accompanying text.

114. Bianchini, *supra* note 103, at 7.

meters, ultimately concluding that the use of private smart meter data for law enforcement purposes does implicate Fourth Amendment protections. It closes by using information-privacy cases of *Whalen v. Roe* and *NASA v. Nelson* to consider the constitutional reasonableness of smart meter data collection for non-law enforcement purposes, such as when the government is acting in the role of a public utility.

Smart meters highlight a growing tension in this area. The normal Fourth Amendment intuition is that you, as an individual, have no expectation of privacy in the records of companies with which you do business.[115] Yet at the same time, a growing body of Fourth Amendment case law has softened previously fixed antiprivacy rules in the face of advancing technology and the increasing ease with which a significant amount of intimate data can be collected.[116] And, with smart meters, there is the additional complication of the role of the home, which is traditionally the most protected physical location for Fourth Amendment purposes.[117] Though this Article's ultimate focus is broader than government information gathering, the standards of the Fourth Amendment help illuminate the fundamental challenge of smart meter—and general smart home—technology.

An important nuance in the energy domain is the multiple roles that the government may play. In the United States, there are both privately owned utilities, which include investor-owned utilities and rural electric-cooperative associations, and publicly owned utilities, which include federal power systems such as the Tennessee Valley Authority and public power systems such as the Los Angeles Department of Water and Power.[118] The Fourth Amendment only applies directly to publicly owned utilities, which have been estimated to make up about 67% of the utilities in the United States but only serve about 15% of electric customers.[119] Private investor-owned utilities are primarily regulated by

115. *See* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

116. *See generally, e.g.*, *id.* (protecting cell phone location records); Riley v. California, 573 U.S. 373 (2014) (protecting cell phones from warrantless searches); United States v. Jones, 565 U.S. 400 (2012) (prohibiting the installation of a GPS tracker on a private vehicle).

117. *See* Jonathan L. Hafetz, *"A Man's Home Is His Castle?": Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries*, 8 WM. & MARY J. WOMEN & L. 175, 175–76 (2002).

118. *See* EISEN ET AL., *supra* note 25, at 71–72; *Differences Between Publicly and Investor-Owned Utilities*, CAL. ENERGY COMMISSION, https://ww2.energy.ca.gov/pou_reporting/background/difference_pou_iou.html [https://perma.cc/52W2-XPRF].

119. *See Stats and Facts*, AM. PUB. POWER ASS'N, https://www.publicpower.org/public-power/stats-and-facts [https://perma.cc/6BY8-EVZG]; *Today in Energy*, U.S. ENERGY INFO. ADMIN. (Aug. 15, 2019), https://www.eia.gov/todayinenergy/detail.php?id=40913 [https://perma.cc/ZD77-8AGL].

state public-utility commissions, but privacy regulations can vary dramatically state by state.[120]

Depending on where one lives, therefore, one's energy provider might be a government entity—a public or semi-public utility—or a private corporation. If the utility is a private company, then the Fourth Amendment question is whether you have an expectation of privacy in that company's records. This implicates the "third-party doctrine." If the utility is public, however, then two separate questions arise: First, whether the government can insist on the installation of a smart meter on a home—the meter itself could be a Fourth Amendment search—and, second, whether there is a Fourth Amendment problem with the "utility" portion of the government sharing information with the "law enforcement" portion of the government. We believe that the ultimate Fourth Amendment answer should be the same for public and private utilities—that people do have an expectation of privacy in energy-usage records and that the government should be required to obtain a warrant if it wishes to access those records for law enforcement purposes. But we shall begin with the private-utility case before complicating our analysis by considering the implications of a public utility.

A. *The Third-Party Doctrine*

The Fourth Amendment guarantees the people's right to be free from "unreasonable searches and seizures."[121] The current test for whether a particular investigative action implicates the Fourth Amendment is given in Justice John Harlan's concurrence to *Katz v. United States*.[122] This test requires that the person being searched by the police have a subjective expectation of privacy in the place or thing being searched and that this expectation be objectively reasonable.[123] Once it is determined that a search implicates the Fourth Amendment, a court then must determine if the search or seizure is itself reasonable, thus reasonableness enters the analysis twice.[124] In the law enforcement context, the search of a private space for law enforcement purposes is reasonable if the government agent has a warrant from an independent magistrate or if one of the numerous exceptions to the warrant requirement applies.[125]

The Fourth Amendment has historically granted no protection for information that people voluntarily share with third parties, including not only friends but also private companies.[126] The government's acquisition

120. *See, e.g.*, *Differences Between Publicly and Investor-Owned Utilities*, *supra* note 118.
121. U.S. CONST. amend. IV.
122. 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
123. *See id.* at 361.
124. *See, e.g.*, Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 187–88 (2004).
125. *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).
126. United States v. Miller, 425 U.S. 435, 443 (1976).

of this information is not considered a "search" for Fourth Amendment purposes and therefore courts do not even reach the question of whether the acquisition is reasonable; the information is treated as having been completely nonsecret.[127] In its most basic form, this "third-party doctrine" is unexceptional. Police informants and coconspirators-turned-informants regularly reveal information to the government that was entrusted to them by another. In the words of Justice Potter Stewart writing in the seminal case of *Hoffa v. United States*,[128] "Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[129] Thus, the law assumes that as soon as you impart a private piece of information to another, it is no longer considered private information under the Fourth Amendment.

Though few object to the idea of allowing criminals to betray their former confederates, support for the third-party doctrine frays substantially when the same principle is applied to the business records that law-abiding companies hold on criminal suspects.[130] And it is easy to see why this application is controversial. The doctrine removes from Fourth Amendment protection huge swathes of otherwise private data that is collected by private companies on a regular basis. Were the traditional third-party doctrine to govern smart meter data, then the government could freely obtain this type of data from private utilities without a warrant.

The origins of the business-records portion of the third-party doctrine can be found in two cases where the Supreme Court found no reasonable expectation of privacy in information recorded and stored by a private company. First, the Court in *United States v. Miller*[131] held that there is no reasonable expectation of privacy in financial documents held by a bank.[132] "All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[133] The depositors, the Court said, assume the risk that the bank

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

128. 385 U.S. 293 (1966).

129. *Id.* at 302; *see also* Lopez v. United States, 373 U.S. 427, 465 (1963) (Brennan, J., dissenting in regards only to electronic eavesdropping) ("The risk of being overheard by an eavesdropper or betrayed by an informer . . . is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak.").

130. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009) (describing the third-party doctrine as "the *Lochner* of search and seizure law, widely criticized as profoundly misguided" (footnote omitted)).

131. 425 U.S. 435 (1976).

132. *See id.* at 440–42.

133. *Id.* at 442.

will reveal their affairs to the government upon request.[134] The innocent bank, like the guilty coconspirator, is perfectly free to expose the secrets of those who trusted it with their private financial information. Similarly, the Supreme Court found in *Smith v. Maryland*[135] that individuals have no reasonable expectation of privacy in the numbers dialed from their home telephones and thereby possessed by the telephone companies.[136] Again, the Court treated the private company as a potential informer, free to share its records with the government.[137]

The timeline of this doctrine is interesting. The original informer cases were decided in the 1960s, and *Smith* and *Miller* are creations of the 1970s. Much has changed since then. The amount and granularity of personal information that is collected by new forms of technology provides a significantly more intimate picture of individuals and their activities than did the technologies and habits of even two decades ago. The potential applications of the third-party doctrine are enumerable in modern society, especially with the addition of more devices that are used on an hourly basis. More and more commercial companies are recognizing the value in home energy-consumption data as a means of gathering information about their current and potential customers.

The Supreme Court has not been blind to this digital revolution. The first truly qualitative shift in the Supreme Court's Fourth Amendment jurisprudence in response to this development came in *Riley v. California*,[138] which held that a cell phone cannot be searched incident to arrest absent a warrant or generally recognized exception to the warrant requirement.[139] Existing case law had been read to allow warrantless searches of any and all physical containers in the arrested persons' possession—items such as purses, wallets, and briefcases—incident to arrest.[140] So arrested persons could expect a warrantless search of any personal papers that they were carrying, including opened mail, notes from old friends, and the like. And, before *Riley*, federal appellate courts frequently upheld warrantless searches of cell phones incident to arrest.[141]

---

134. *See id.* at 443.

135. 442 U.S. 735 (1979).

136. *Id.* at 742.

137. *See id.* at 744–45.

138. 573 U.S. 373 (2014).

139. *Id.* at 393 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person.").

140. *See* United States v. Robinson, 414 U.S. 218, 236 (1973) (contents of a cigarette pack); United States v. Carrion, 809 F.2d 1120, 1123, 1128 (5th Cir. 1987) (billfold and address book); United States v. Watson, 669 F.2d 1374, 1383–84 (11th Cir. 1982) (wallet); United States v. Lee, 501 F.2d 890, 892 (D.C. Cir. 1974) (purse).

141. *See, e.g.*, United States v. Curtis, 635 F.3d 704, 711–13 (5th Cir. 2011); United States v. Murphy, 552 F.3d 405, 411–12 (4th Cir. 2009); United States v. Finley, 477 F.3d 250, 259–60

In *Riley*, Chief Justice John Roberts likened the argument that cell phones were "materially indistinguishable" from briefcases to "saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."[142] Cell phones simply contained too much information to treat them like physical papers.[143] So the Court fashioned a bright-line rule: police must "get a warrant" to search a cell phone.[144] This represented a substantial shift in Fourth Amendment law, and it was widely discussed as such in both the scholarly literature and the popular press.[145]

The stakes and torches of this digital revolution reached the palaces of the third-party doctrine just four years later in *Carpenter v. United States*. There, the Supreme Court held that the Fourth Amendment extends to protect historical cell-site location information (CSLI) records from cell phones.[146] These records are generated every time a cell phone connects to a cell tower, which most modern devices will attempt to do several times a minute.[147] The data therefore has the potential to represent a moment-by-moment catalogue of a cell phone user's movements.[148] The police in *Carpenter* had obtained a court order issued under the Stored Communications Act to access the CSLI records, but the Court held that this was insufficient.[149] Even though CSLI is contained in the phone company's own records, a warrant was required to access it.[150]

Chief Justice Roberts's majority in *Carpenter* noted two distinctions from prior case law, both important for this Article's purposes. First, he explained that the conveyance of location information to cell phone

(5th Cir. 2007); *see also* United States v. Flores-Lopez, 670 F.3d 803, 809–10 (7th Cir. 2012) (permitting a limited cell phone search incident to arrest, while reserving the question of whether a more invasive search would have been permissible without a warrant).

142. *Riley*, 573 U.S. at 393.

143. *See id.* ("Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.").

144. *Id.* at 403.

145. *See, e.g.*, Matthew B. Kugler & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. CHI. L. REV. 1747, 1771–74 (2017); Paul Ohm, *The Life of Riley (*v. California*)*, 48 TEX. TECH L. REV. 133, 133, 134 (2015) (describing *Riley* as a "significant milestone in constitutional criminal procedure" and a "privacy opinion for the ages"); Orin Kerr, *The Volokh Conspiracy: The Significance of* Riley, WASH. POST (June 25, 2014, 11:56 AM), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/25/the-significance-of-riley/?utm_term=.d867005e9b0b [https://perma.cc/M3TF-W4J3] ("*Riley* can be fairly read as saying that computers are a game-changer: We're now in a 'digital age,' and quantity of data and the 'qualitatively different' nature of at least some digital records changes how the Fourth Amendment should apply.").

146. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

147. *Id.* at 2211.

148. *See id.*

149. *Id.* at 2221.

150. *See id.*

providers was not really "voluntary" because it did not require any affirmative act on the part of users "beyond powering up"[151] and cell phones are now a ubiquitous part of daily life; carrying one is "indispensable to participation in modern society."[152] So, in Chief Justice Roberts's view, any exposure of information that comes from merely carrying a phone is not truly voluntary as one cannot dispense with the "indispensable."

Second, Chief Justice Roberts placed great importance on the uniquely revealing nature of historical CSLI. Some forms of data are so "detailed, encyclopedic, and effortlessly compiled" that additional protections under the Fourth Amendment are required.[153] CSLI has the potential to reveal many of the privacies of life, including issues of great personal intimacy.[154] He also recognized that accessing a person's historic CSLI records presented "even greater privacy concerns" than prospective GPS monitoring because historical CSLI records give the government near-perfect location surveillance on a person, subject only to the five-year retention policies of most wireless carriers.[155] Though CSLI was undoubtedly useful to law enforcement, "this tool risks Government encroachment of the sort the Framers, 'after consulting the lessons of history,' drafted the Fourth Amendment to prevent."[156]

This holding represented a sharp break from prior third-party doctrine jurisprudence, a point made vigorously in dissent by Justice Anthony Kennedy. He pointed out that, whatever the sensitivity of historical location data, the information at issue was fundamentally in records owned and controlled by a third party.[157] He therefore would have treated the case as bound squarely by *Smith* and *Miller*, precedents that the majority notably did not overturn.[158] He also challenged the notion that

151. *Id.* at 2220.

152. *Id.*

153. *See id.* at 2216–17.

154. *See* Riley v. California, 573 U.S. 373, 396 (2014) (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)); *see also Jones*, 565 U.S. 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.").

155. *Carpenter*, 138 S. Ct. at 2218; *see also id.* at 2223 ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.").

156. *Id.* at 2223 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

157. *See id.* at 2231 (Kennedy, J., dissenting) ("Cases like this one, where the Government uses court-approved compulsory process to obtain records owned and controlled by a third party, are governed by the two majority opinions in *Miller* and *Smith*.").

158. *Id.*

CSLI was uniquely revealing.[159] A person's movements are, after all, generally in public spaces. Financial and telephone records, by contrast, might reveal more:

> What persons purchase and to whom they talk might disclose how much money they make; the political and religious organizations to which they donate; whether they have visited a psychiatrist, plastic surgeon, abortion clinic, or AIDS treatment center; whether they go to gay bars or straight ones; and who are their closest friends and family members.[160]

This evolution of the third-party doctrine complicates the story for smart meter data in the hands of private companies. Twenty years ago, it would have been easy to argue that energy-consumption information, which is collected by utilities and is an essential part of their operations, is merely a collection of business records.[161] The electricity bill is only one of many that is paid out of the family checking account, and *Miller* teaches that even the totality of the family accounts can be examined absent a warrant.[162] The U.S. Court of Appeals for the Ninth Circuit reached exactly that conclusion on exactly that reasoning as recently as 2012.[163] "The records sought here are business records owned and possessed by [the utility]" and "[the utility's] business records are no more inherently personal or private than the bank records in *Miller*."[164] And the U.S. Court of Appeals for the Eighth Circuit came to the same conclusion in 2011.[165] In both the Eighth and Ninth Circuit cases, the underlying investigation was drug related.[166]

But then the world changed. Part of that change is the introduction of smart meters. Suddenly they generate information hour by hour or minute by minute rather than month by month. And part of the change is in the legal rule. After *Carpenter*, the question is whether smart meter data is sufficiently involuntarily conveyed, sufficiently revealing, and

159. *See id.* at 2234 ("But the Court does not explain what makes something a distinct category of information.").

160. *Id.* at 2232.

161. *See* State v. Kluss, 867 P.2d 247, 252 (Idaho Ct. App. 1993) (finding no expectation of privacy in utility records under federal or state constitutions).

162. United States v. Miller, 425 U.S. 435, 437–40 (1976).

163. *See* United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1116 (9th Cir. 2012).

164. *Id.*

165. *See* United States v. McIntyre, 646 F.3d 1107, 1111–12 (8th Cir. 2011) ("Similarly, when [McIntyre] used power in his home, he voluntarily conveyed that information to [Cedar–Knox Public Power District]." (alterations in original) (quoting United States v. Hamilton, 434 F. Supp. 2d 974, 979 (D. Or. 2006))).

166. *See Golden Valley*, 689 F.3d at 1111; *McIntyre*, 646 F.3d at 1110.

sufficiently unique to the new digital world to warrant becoming the second exception to the third-party doctrine.

B. *Electronic Infiltration of the Home*

When considering whether smart meter data is sufficiently special to qualify for an exception to the third-party doctrine, we must consider the role of the home in modern Fourth Amendment law. Despite the Supreme Court's assertion in *Katz* that "the Fourth Amendment protects people, not places,"[167] emphasis has often been placed on the home. The home has been viewed as an especially private space by American privacy law since its founding. The Fourth Amendment was in part a response to British excesses such as "general warrants" and "writs of assistance" in the colonies,[168] which allowed people and their homes to be searched without cause to believe they had committed an offense. Forced entry into a home and "rummaging around inside were understood as the paradigmatic examples of 'searches.'"[169]

This focus on location and, particularly, on the home has caused complications in several cases involving technological surveillance. In two cases from the 1980s, police officers installed electronic trackers (beepers) in containers of chemicals used in the production and processing of illegal drugs.[170] Informants then sold those containers to suspected drug dealers so that the government could trace where the suspects had established their drug labs.[171] In the first case, *United States v. Knotts*,[172] the officers tracked the property when it was in the suspect's car traveling over public roads.[173] Ultimately, the container came to rest in a secluded cabin, which the police then raided.[174] In the second case, *United States v. Karo*,[175] the officers tracked the container through three houses and two storage facilities.[176]

---

167. Katz v. United States, 389 U.S. 347, 351 (1967).

168. *History and Scope of the Amendment: Search and Seizure: Fourth Amendment*, JUSTIA, https://law.justia.com/constitution/us/amendment-04/01-search-and-seizure.html [https://perma.cc/Z7WX-RW84] ("In order to enforce the revenue laws, English authorities made use of writs of assistance, which were general warrants authorizing the bearer to enter any house or other place to search for and seize 'prohibited and uncustomed' goods, and commanding all subjects to assist in these endeavors.").

169. Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 72.

170. *See* United States v. Karo, 468 U.S. 705, 708 (1984); United States v. Knotts, 460 U.S. 276, 277–78 (1983).

171. *See Karo*, 468 U.S. at 708; *Knotts*, 460 U.S. at 278.

172. 460 U.S. 276 (1983).

173. *Id.* at 281.

174. *Id.* at 278–79.

175. 468 U.S. 705 (1984).

176. *Id.* at 708–09.

In *Knotts*, the beeper tracking did not present a Fourth Amendment problem.[177] Though the final destination was on private property, the beeper's transit occurred entirely over public roads and so, to the Court, was therefore exposed to public view.[178] The use of the beeper to track the location had been practically necessary—the police had difficulty monitoring the suspect's car given his "evasive maneuvers"—but there was no inherent reason why naked-eye surveillance could not have obtained the same information.[179] The Court later found distinguishable facts in *Karo,* however. There, the police repeatedly used the beeper to determine whether the incriminating container was still present in a private residence, a fact that they were having great difficulty otherwise observing.[180] Though "[t]he monitoring of an electronic device such as a beeper is, of course, less intrusive than a full-scale search, but it does reveal a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant."[181]

This seems a somewhat curious distinction. One leaves a private residence on public roads, so the question of whether one is still in a house can generally be answered by watching the outside. But the Court was balancing two strong intuitions. The first is that public roads are generally public.[182] The second is plainly expressed in *Karo*: "*At the risk of belaboring the obvious*, private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable."[183] And, several pages later, the Court noted that "[i]ndiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."[184]

The very act of carrying the electronic surveillance device over the threshold into a private building, then, changes the character of its use. Checking the beeper *before* the container is carried into a building is perfectly permissible; you are tracking an object in public spaces. But, checking the beeper *after* to determine if it is still in the building is not permissible; you are monitoring a private space. A space so private, in fact, that it is "obvious" that the Fourth Amendment protects it.

---

177. *Knotts*, 460 U.S. at 285.

178. *Id.* at 281–82.

179. *Id.* at 278, 285.

180. *Karo*, 468 U.S. at 714–15.

181. *Id.* at 715.

182. *Knotts*, 460 U.S. at 281 ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

183. *Karo*, 468 U.S. at 714 (emphasis added).

184. *Id.* at 716.

The Supreme Court similarly recognized the importance of protecting homes from enhanced surveillance made possible by advancing technology in *Kyllo v. United States*.[185] There the Court held that the government cannot use a thermal imager outside of a home to explore what is happening inside the home because doing so would leave homeowners "at the mercy of advancing technology."[186] At the time of the Court's decision, thermal imagers were not widely used by the public.[187] The Court found that the simple act of collecting thermal images of the home while standing outside of it constituted a search under the Fourth Amendment even if the person observing the home did not enter the property.[188]

The technology used in *Kyllo* was fairly primitive.[189] "The scan showed that the roof over the garage and a side wall of petitioner's home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex."[190] This was useful for detecting use of halide lights in a marijuana farm but did not reveal much about the other activities of the home's occupants.[191] Nevertheless, the Court looked ahead at technologies then being developed which might allow thermal imaging "through-the-wall" and would therefore reveal the movements of people inside a house.[192] Thinking of what technology would potentially soon enable substantially eased the majority's decision.

C. *The Fourth Amendment and Private Smart Meter Data*

The forward-looking concern evident in *Kyllo* returns us to smart meters. First consider the common case where a private utility has information about electricity consumption and the government wants to obtain that information for law enforcement purposes. As discussed in Part I, smart meters can convey a significant amount of information about the activities that occur within a home if the data is properly disaggregated. "Granular AMI data presents a potential new tool for law enforcement to investigate a much broader set of crimes or even track people's whereabouts."[193] Even given the current state of the technology,

185. 533 U.S. 27, 35–36 (2001).

186. *Id.*

187. *See id.* at 40. The holding seemed to rest primarily on the public's access to advanced technology but also recognized the importance of protecting the home. *Id.* ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").

188. *See id.*

189. *See id.* at 36 ("[T]he technology used in the present case was relatively crude . . . .").

190. *Id.* at 30.

191. *See id.*

192. *See id.* at 36.

193. Harvey, *supra* note 10, at 2082.

it is already possible to tell a fair amount about household occupancy patterns, and tech companies are working hard to connect smart devices together.[194] As technology advances and more devices are directly linked to smart meters, the ability of utilities and potentially other companies to deduce a family's behaviors in the home will only increase. As one writer put it, "[T]he digitization of just about everything is not just possible but likely, and that now is the time to be freaking out about the dangers."[195]

The central tenet in Fourth Amendment law is "the right of a man to retreat into his own home and there be free from unreasonable government intrusion."[196] A person's expectation of privacy is highest in the home, but smart meters risk exposing intimate details of daily life simply by gathering energy-consumption data in small intervals of time. In *Kyllo*, the Supreme Court started in the right direction by stating that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search."[197] Noting that "the Fourth Amendment draws 'a firm line at the entrance to the house,'" the Court reaffirmed that line by requiring a "clear specification of those methods of surveillance that require a warrant."[198]

In one sense, smart meters fit well within the bounds of *Kyllo*; they are a new technology that allows for the cataloging and potential surveillance of intimate details within the home. And, unlike *Kyllo*, the privacy-penetrating possibilities of this technology are already realized. Even current smart meter data tells you quite a lot about a household.[199] *Kyllo*, however, emphasized that the technology in question was not in "general public use,"[200] and smart meters are increasingly common by contrast. Utilities often either mandate smart meter installation or make it quite difficult to opt out of it, so the share of customers using smart meters can only be expected to increase.[201] But as the near-compulsory

194. Farhad Manjoo, *A Future Where Everything Becomes a Computer Is as Creepy as You Feared*, N.Y. TIMES (Oct. 10, 2018), https://www.nytimes.com/2018/10/10/technology/future-internet-of-things.html?emc=edit_nn_20181011&nl=morning-briefing&nlid=85811686201810 11&te=1 [https://perma.cc/Q2RF-UYFA] ("Cars, door locks, contact lenses, clothes, toasters, refrigerators, industrial robots, fish tanks, sex toys, light bulbs, toothbrushes, motorcycle helmets—these and other everyday objects are all on the menu for getting 'smart.'").

195. *Id.*

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

197. Kyllo v. United States, 533 U.S. 27, 34 (2001) (citation omitted) (quoting *Silverman*, 365 U.S. at 512).

198. *Id.* at 40 (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).

199. *See supra* Part I.

200. *Kyllo*, 533 U.S. at 34.

201. Duarte, *supra* note 14, at 1154 ("In many places, smart meter adoption is all but compulsory. Utility companies typically inform the consumer that a smart meter will be installed and then send an employee to install the meter.").

nature of smart meter installation brings this issue somewhat away from *Kyllo*, it drops it squarely into the bounds of *Carpenter*.

For many in the United States, smart meters are installed as part of mandatory utility upgrades.[202] Though some states require that utilities allow customers to "opt out" of smart meter installation, the utilities can and do charge one-time fees or monthly fees that can be prohibitively expensive.[203] Some utilities, such as Commonwealth Edison (ComEd), which serves the greater Chicago area, do not allow for permanent opt outs and only permits consumers to pay to delay the installation of the smart meter.[204] Moreover, when consumers move residences or purchase new homes, it is unlikely that they will reach out to the utility to have an already-installed smart meter removed, and many utilities would charge consumers to have the meters switched out.[205] Further, consumers are often unable to switch their electricity provider due to the regional monopoly structure of public utilities in much of the United States.[206] Many electricity customers are "captive customers" and must use the public utility in their geographic area or go without electricity, which is not really an option in the twenty-first century.[207]

Carpenter does not lay out a clear test for when to look beyond the third-party doctrine and grant Fourth Amendment protection to an individual's personal data. Orin Kerr, the year after *Carpenter*, understood it as proposing a three-step test.[208] First, the business records in question must be new to the "digital age."[209] Second, the records must

---

202. *See id.* at 1153–54.

203. *Smart Meter Opt-Out Options and Fees*, ELECTRONIC SILENT SPRING, http://www.electronicsilentspring.com/wp-content/uploads/2014/01/SMART-METER-OPT-OUT-OPTIONS-AND-FEES-by-STATE.pdf [https://perma.cc/AU2A-5AZY] (last updated Nov. 6, 2016) (explaining, for example, in California, Sacramento consumers must pay a one-time fee of $127 in addition to $14 per month to have their analog meter read by the utility company).

204. *See id.*

205. *See* W. MONROE PARTNERS, AMI OPT-OUT: POLICIES, PROGRAMS AND IMPACTS ON BUSINESS CASES (2015), https://www.westmonroepartners.com/-/media/Files/White-Papers/West-Monroe-Partners-AMI-Opt-Out-White-Paper-62012.pdf [https://perma.cc/8H4G-6ZNW] (demonstrating that there are many different ways that utilities provide for customers to opt out including charging customers a monthly fee for continued use of their analog meter); *Smart Meter Opt-Out Options and Fees*, *supra* note 203 (illustrating that several utilities, including Duke Energy Ohio, charge money for replacing the smart meter with an analog meter and then also charge for monthly analog meter readings).

206. *See* David Roberts, *Power Utilities Are Built for the 20th Century. That's Why They're Flailing in the 21st.*, VOX (Sept. 9, 2015, 9:10 AM), https://www.vox.com/2015/9/9/9287719/utilities-monopoly [https://perma.cc/9JKB-SNP5].

207. *See id.*

208. Orin S. Kerr, *Implementing* Carpenter (USC Law Legal Studies, Working Paper No. 18-29, 2018) (manuscript at 3), https://ssrn.com/abstract=3301257 [https://perma.cc/2VKD-A2E9].

209. *See id.*

be created without "meaningful voluntary choice."[210] And, third, "the records must tend to reveal 'the privacies of life.'"[211] Steps two and three of Kerr's framework appear to be inherent in the language of *Carpenter*; Chief Justice Roberts spent a great deal of time discussing voluntariness and exposure risk.[212] And, on these steps, smart meters would likely trigger Fourth Amendment protection. If going without a cell phone is not considered a viable way of avoiding the collection of cell phone location data, then going without power is not a viable way of avoiding the collection of smart meter data.[213] Similarly, if smart meter data can show at least "when you are at home and when you are away, when you lie down and when you rise,"[214] that likely qualifies as the "privacies of life."

The first requirement—that the records be new to the digital age or substantially transformed by it—is less clear. Kerr explains this step as requiring that "[t]he records must be of a kind and nature that generally could not be collected in a pre-digital age. Pre-digital records and their modern equivalents are exempt, sort of like a constitutional grandfather clause."[215] He points to language from Chief Justice Roberts's majority opinion referring to "seismic shifts in digital technology that [have] made possible"[216] access to "an entirely different species"[217] of data that "do[] not fit neatly under existing precedents."[218]

We fear that one can plausibly argue that almost all types of records have been substantially transformed by the digital age, making this prong of the test somewhat useless. Have bank statements been substantially transformed by the digital age? Arguably, yes. Credit cards as we now understand them were only introduced in the 1950s.[219] Electronic processing of credit card payments only began in the 1970s.[220] It was only in 1986 that Visa launched an ad campaign trumpeting its evolution "from a travel and business tool to a card for everyday use."[221] In 1970, only 16% of families had a bank-type credit card, such as Visa or

210. *Id.*

211. *Id.* (manuscript at 22).

212. *Id.* (manuscript at 20–21).

213. *See supra* notes 151–152 and accompanying text.

214. *Deuteronomy* 6:7 (New Revised Standard Version).

215. Kerr, *supra* note 208 (manuscript at 16).

216. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

217. *Id.* at 2222.

218. *Id.* at 2214.

219. *See History of Credit Card Processing*, BEBUSINESSED.COM, https://bebusinessed.com/history/history-of-credit-card-processing/ [https://perma.cc/N4SS-WSM6].

220. *Id.*; *see* Claire Tsosie, *What the First Credit Cards Were Like*, FORBES (Aug. 29, 2016, 12:27 PM), https://www.forbes.com/sites/clairetsosie/2016/08/29/what-the-first-credit-cards-were-like/#2f051835ec9a [https://perma.cc/LA4Y-WGFN].

221. *History of Visa: Our Journey*, VISA, https://usa.visa.com/about-visa/our_business/history-of-visa.html [https://perma.cc/9QDC-PJZR].

Mastercard.[222] By 1998, 68% of families had such a card.[223] Nationwide, a 2017 survey suggested that only a quarter of *in-store* purchases are now completed using cash—online purchases are, of course, virtually never conducted with cash.[224] Many law students at Northwestern University say that they do not even carry cash on a regular basis. This means that every transaction conducted by these students is directly reflected in the records of a financial institution. A bank knows when and where they got their morning coffee, how often they buy lunch rather than pack it, and which friend they Venmo for their share of the bar tab after class. *Miller*, which found no expectation of privacy in bank records, was decided in 1976.[225] The world of bank records has substantially changed in the intervening years.

Bank statements are only one example of how easy it is to argue that "old" data is now "new" data. Kerr himself makes a similar point about the metadata of Facebook messages and texts, arguing that *Carpenter* requires protection for them despite the clear holding of *Smith* for telephone metadata.[226] We agree that the *Carpenter* exception should apply in this context, but this portion of Kerr's (and Chief Justice Roberts's) test is either so easily satisfied, or so arbitrarily judged, that it is rarely going to be useful. Nevertheless, smart meters are products of the digital revolution; they have only been in widespread use for about a decade.[227] And smart meters convey far more information than did the old analog meters. If one assumes an analog meter is read once a month, then a digital meter being read every fifteen minutes conveys approximately 2,880 times as much information.[228] If anything is new to the digital age and transformed by it, these records are.

As with cell-site location data, the collection of smart meter data from private utilities also likely implicates the Fourth Amendment. The

---

222. *See* Thomas A. Durkin, *Credit Cards: Use and Consumer Attitudes, 1970–2000*, FED. RES. BULL., Sept. 2000, at 623, 625 n.3, 625 fig.1. Technically the names Visa and Mastercard came later, but the brand predecessors were active in 1970. *See, e.g.*, Jeremy M. Simon, *Visa: A Short History*, CREDITCARDS.COM (Mar. 30, 2007), https://www.creditcards.com/ credit-card-news/history-of-visa-1273.php [https://perma.cc/B88L-2SXL].

223. Durkin, *supra* note 222.

224. TSYS, 2017 U.S. CONSUMER PAYMENT STUDY 40 (2018). One could conduct online purchases via cash, check, or money order were one to send payment via mail. This would require the purchaser to be able to find a stamp, however, and this is well-known to be impossible.

225. *See* United States v. Miller, 425 U.S. 435, 440–42 (1976).

226. Kerr, *supra* note 208 (manuscript at 43–45) (arguing that "[f]or today's teenagers, texting is like speaking" due to the sheer number of texts sent in a day).

227. *See* T. Wang, *Number of Electric Smart Meters Installations Deployed in the U.S. from 2007 to 2020 (in million units)*, STATISTA, https://www.statista.com/statistics/676472/number-of-smart-meter-installations-in-the-united-states/ [https://perma.cc/8NWV-2S5P] (showing that approximately 7 million smart meters had been installed in the United States by the end of 2007 and that 72 million had been installed by the end of 2016).

228. With four readings per hour in a thirty-day month, there are 2,880 readings per month.

Supreme Court should follow its reasoning in *Kyllo* and *Carpenter* when considering how to protect smart meter data and should reject the application of the third-party doctrine to it. Ultimately, the risk posed by technological advancements and the interconnection of smart meters to the internet of devices within the home is too high and therefore smart meter data should be provided additional protections.

D. *Reasonableness Balancing and Public Utilities*

All *Carpenter* and *Kyllo* establish, however, is that the Fourth Amendment is implicated—that collection of smart meter data is a search—even if that data is in the hands of a third-party corporation and not held by the consumer. This still leaves two further questions. First, is the collection of smart meter data an "unreasonable" search? Recall that reasonableness enters the Fourth Amendment analysis twice, once in deciding whether something is a search—reasonable expectations of privacy—and then in evaluating whether that search is permissible without a warrant.[229] Second, what about when the government is the utility? Many utilities in the United States are government owned or operated.[230] Is it a Fourth Amendment problem to mandate the collection of smart meter data?

In *Carpenter*, the Supreme Court rapidly stepped from the conclusion that the Fourth Amendment was implicated—that the collection of several days of historical cell-site data was a search—to the conclusion that only a warrant based upon probable cause could justify the transfer of that information to the government for use in a criminal investigation. "Although the 'ultimate measure of the constitutionality of a governmental search is "reasonableness,"' our cases establish that warrantless searches are typically unreasonable where 'a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing.'"[231] The *Carpenter* Court has been criticized for the speed of this jump. For instance, Alan Rozenshtein commented that the Court reached this conclusion "[w]ithout much analysis."[232] He would have preferred a contextual reasonableness analysis for the protection of *Carpenter*-style third-party data, with substantial deference to legislative judgements, rather than a flat warrant rule.[233]

We see no reason to quarrel with the traditional warrant rule in either the smart meter or cell site data contexts; *Carpenter* is on firm doctrinal

229. *See supra* notes 121–125 and accompanying text.

230. *See supra* notes 118–120 and accompanying text.

231. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652–53 (1995)).

232. Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J.F. 943, 946 (2019).

233. *See id.* at 954–60.

ground in making the leap from the implication of the Fourth Amendment to a warrant requirement when the purpose of the data collection is law enforcement use.[234] So this settles the case of the government requesting energy-consumption data from a private utility for law enforcement purposes. But this reasonableness question is more complicated when considering government utilities. Is it a search for a government, such as a publicly owned utility, to install a smart meter and, if so, is the search of the energy-usage data reasonable? Or, put another way, what kinds of protections are required to make such a search reasonable?

Consideration of the Fourth Amendment implications of public utility smart meter installation goes beyond the criminal law aspects of the Fourth Amendment. In general, the criminal/noncriminal distinction is exceptionally important in the context of the Fourth Amendment. When the government acts as an employer, for instance, it will often have an understandable need to gather information about current and prospective employees. Though this information collection would often require a warrant based upon probable cause in the law enforcement context, reasonable suspicion is often sufficient in the employment domain.

> In contrast . . . public employers are not enforcers of the criminal law; instead, public employers have a direct and overriding interest in ensuring that the work of the agency is conducted in a proper and efficient manner. In our view, therefore, a probable cause requirement for searches of the type at issue here would impose intolerable burdens on public employers.[235]

Similarly, the warrant requirement often does not apply in the public-education context because, again, school officials are not generally enforcers of criminal law.[236]

Based on these precedents, the government may be able to collect smart meter data for utility purposes even if it would require a warrant to do so for law enforcement purposes. The reasonableness balancing that so quickly leads to a warrant requirement in the law enforcement domain will function differently outside of it. To explore this non-law enforcement balancing, it is helpful to consider the constitutional right to information privacy more generally. This right, though based in part in the Fourth Amendment, stems from the traditions of *Griswold v. Connecticut*[237] and *Roe v. Wade*[238] rather than the enforcement of

234. *See, e.g.*, *Vernonia Sch. Dist.*, 515 U.S. at 652–53.

235. O'Connor v. Ortega, 480 U.S. 709, 724 (1987).

236. *See* New Jersey v. T.L.O., 469 U.S. 325, 340 (1985) (holding that "school officials need not obtain a warrant before searching a student who is under their authority").

237. 381 U.S. 479 (1965).

238. 410 U.S. 113 (1973).

criminal law. One case in the information-privacy domain presents a close analogy for smart meters. In *Whalen v. Roe*,[239] the Court evaluated the constitutionality of a New York act requiring reporting and storage of information concerning all Schedule II drug prescriptions.[240] Physicians were required to report the name of "the prescribing physician; the dispensing pharmacy; the drug and dosage; and the name, address, and age of the patient."[241] The district court had struck down the act as an unnecessary intrusion into one of the "zones of privacy accorded constitutional protection."[242]

The Supreme Court overturned the district court.[243] Those challenging the law had argued that doctors would be less willing to prescribe, and patients would be less willing to use, certain drugs given these regulations.[244] The Court, however, held that patients' privacy interests were not grievously impacted because the law's data-security provisions were sufficient to prevent accidental disclosure or inappropriate use of the information.[245] The collection of the information was reasonable given its value to the public in preventing abuse of prescription drugs and the safeguards the government imposed to prevent public release of the data. The limited public-safety purpose, independent of criminal law enforcement, made constitutionally permissible what was otherwise a severe intrusion into a sensitive domain.

Since the Supreme Court upheld New York's information-gathering statute, it is unclear how intrusive a practice must be to violate the right to information privacy, or even whether there is such a freestanding right. Lower courts are split. The U.S. Court of Appeals for the Third Circuit subsequently developed a seven-part test to determine whether the government could acquire records like those at issue in *Whalen*.[246] This test, broadly speaking, balances the magnitude of the privacy invasion (including the harm likely to be inflicted if the data is subsequently released and the extent of the data-security measures) against the extent of the state's interest.[247] The U.S. Courts of Appeals for the Second, Fifth,

239. 429 U.S. 589 (1977).
240. *See id.* at 591, 593.
241. *See id.* at 593.
242. *Id.* at 596.
243. *Id.* at 603–04.
244. *Id.* at 600.
245. *See id.* at 600–02.
246. United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980).
247. *See id.* The factors are: (1) the "type of record requested," (2) "the information it does or might contain," (3) "the potential for harm in any subsequent nonconsensual disclosure," (4) the injury a disclosure would cause to the relationship that generated the record, (5) the "adequacy of safeguards to prevent disclosure," (6) "the degree of need for access," and (7) whether there is a public policy reason or statutory mandate militating toward access. *Id.*; *see also* Doe v. Se. Pa.

Seventh, and Ninth Circuits have all also recognized the right in some form,[248] but the U.S. Courts of Appeals for the Sixth Circuit has been more cautious and the U.S. Court of Appeals for the District of Columbia Circuit has questioned whether there is a constitutional right to information privacy at all.[249]

The Supreme Court's only other major return to the constitutional right to information privacy sheds further light on how to think of the "government as utility" question. In *NASA v. Nelson*,[250] the Supreme Court considered the constitutionality of the government asking intrusive questions in its background checks in its capacity as an employer.[251] The expanded background check at issue in *Nelson* was moderately invasive, inviting commentary on a potential contractor's medical status, criminal history, financial stability, and interpersonal relationships.[252] Private employers often inquire into a broad range of deeply personal topics as part of their hiring processes, so this was not out of step with industry practices.[253]

The Court held that these inquiries were constitutionally permissible.[254] It emphasized that the government has a "much freer hand" when acting in its capacity as an employer than it does when it "brings its sovereign power to bear on citizens at large."[255] It could make the same sorts of inquiries that a private employer would, and these questions were very common in the private sector.[256] The open-ended

---

Transp. Auth., 72 F.3d 1133, 1135–38 (3d Cir. 1995) (applying this test to the disclosure of an employee's HIV status).

248. *See, e.g.*, Coffman v. Indianapolis Fire Dep't, 578 F.3d 559, 566 (7th Cir. 2009); *In re* Crawford, 194 F.3d 954, 959 (9th Cir. 1999); Barry v. City of New York, 712 F.2d 1554, 1559 (2d Cir. 1983); Fadjo v. Coon, 633 F.2d 1172, 1176 (5th Cir. 1981).

249. *See* J.P. v. DeSanti, 653 F.2d 1080, 1089–90 (6th Cir. 1981) ("We do not view the discussion of confidentiality in *Whalen v. Roe* as . . . creating a constitutional right to have all government action weighed against the resulting breach of confidentiality."); Am. Fed'n of Gov't Emps. v. Dep't of Hous. & Urban Dev., 118 F.3d 786, 791 (D.C. Cir 1997).

250. 562 U.S. 134 (2011).

251. *Id.* at 138.

252. *See id.* at 140–42. The applicants themselves were asked standard biographical and work-history information as well as whether they had used, supplied, or manufactured illegal drugs in the preceding year. *Id.* at 141. The applicants' references, however, were asked an extensive range of open-ended questions. *Id.* at 141–42. One question asked whether the reference had "any reason to question" the employee's "honesty or trustworthiness" and another whether the reference knew of any "adverse information" concerning the employee's "'violation of the law,' 'financial integrity,' 'abuse of alcohol and/or drugs,' 'mental or emotional stability,' 'general behavior or conduct,' or 'other matters.'" *Id.* at 141–42.

253. *See* Stephen F. Befort, *Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place*, 14 HOFSTRA LAB. L.J. 365, 381–400 (1997) (describing the types of information that employers can and do collect).

254. *Nelson*, 562 U.S. at 151–52.

255. *Id.* at 148 (quoting Engquist v. Or. Dep't of Agric., 553 U.S. 591, 598 (2008)).

256. *See id.* at 155.

questions, then, were justifiable as a reasonable measure "aimed at identifying capable employees who [would] faithfully conduct the Government's business" and for separating strong and weak candidates.[257]

Taking *Nelson* seriously suggests that the government, as a utility, should be allowed to collect all the same kinds of information that a private utility would. The government, wearing its utility hat, has valid need of that information and it is not unreasonable for the government to collect information regularly collected by private parties. But taking *Whalen* seriously means that the government incurs special obligations when it uses its "utility hat" to justify the collection of personal information. It must constantly seek to balance its legitimate need for the information—both its need as an actor in the national marketplace and its need as a promoter of the public good—with the privacy concerns of those whose data it is collecting. And the government must be conscious of a key difference from *Nelson*. In that case, people were freely choosing to enter an employment relationship with the government and therefore give to the government all the information that they would normally give to an employer. People are often not freely choosing to have smart meters installed.

Only one federal court of appeals—the Seventh Circuit—has wrestled with the issue of smart meters in the post-*Carpenter* world, and its treatment of reasonableness and government hat wearing is instructive. In *Naperville Smart Meter v. City of Naperville*,[258] a nonprofit organization opposed the city's replacement of the old analog meters with new smart meters, alleging that the city's collection of the smart meter data constituted an unreasonable search under the Fourth Amendment.[259] Since the smart meter initiative was being implemented by a municipal utility, the mere installation of the meters raised Fourth Amendment concerns; the government would receive the energy-consumption reports directly rather than from a third-party utility.[260] Naperville's smart meters collect residents' energy-consumption data every fifteen minutes, the information is stored for up to three years, and residents are unable to opt out of the smart meter program; participation is mandatory.[261]

Considering the voluntariness and exposure prongs of *Carpenter*, the court readily concluded that smart meter data—specifically smart meter

257. *See id.* at 154.
258. 900 F.3d 521 (7th Cir. 2018).
259. *Id.* at 524.
260. *Id.* at 527.
261. *See id.* at 524.

installation—implicated the Fourth Amendment.[262] As the Seventh Circuit recognized, "[I]n this context, a choice to share data imposed by fiat is no choice at all. . . . [A] home occupant does not assume the risk of near constant monitoring by choosing to have electricity in her home."[263] The disclosure of information was therefore neither voluntary nor the result of any affirmative act by the person being surveilled. The Seventh Circuit further noted that smart meters have been adopted "only by a portion of a highly specialized industry," which under *Kyllo*, would make them not in "general public use."[264] This seems somewhat absurd—the highly specialized industry in question being one that is almost universally used. But the court may have been using this analysis to buttress its shift from *Carpenter*'s focus on third-party business records to *Kyllo*'s focus on collection using new technology.

Having easily and, in our view, correctly concluded that the collection of smart meter data by a public utility is a search, the court then assessed whether the search was reasonable.[265] To start, the Seventh Circuit properly considered the benefits that smart meters bring to the city of Naperville.[266] The court noted that "[s]mart meters allow utilities to reduce costs, provide cheaper power to consumers, encourage energy efficiency, and increase grid stability. . . . [T]hese interests render the city's search reasonable, where the search is unrelated to law enforcement . . . and presents little risk of corollary criminal consequences."[267] The court's analysis included consideration of who was collecting the data and for what purpose, and it balanced the interests of those involved.[268] The court noted that "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."[269] It was persuaded by the benefits provided by smart meters and the additional protections afforded the customer data.[270] Notably, the court warned that its holding was limited

262. *Id.* at 525, 527 ("Their data, even when collected at fifteen-minute intervals, reveals details about the home that would be otherwise unavailable to government officials with a physical search. Naperville therefore 'searches' its residents' homes when it collects this data.").

263. *Id.* at 527.

264. *Id.*

265. *Id.* at 528–29.

266. *Id.* at 529.

267. *Id.*

268. *Id.* at 528–29.

269. *Id.* at 528.

270. *Id.* at 528–29 ("Since these searches are not performed as part of a criminal investigation we can turn immediately to an assessment of whether they are reasonable, 'by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate government interests.'" (citation omitted) (quoting Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 187–88 (2004))).

to the particular circumstances of Naperville and that if the data was collected in shorter intervals (more frequently than once every fifteen minutes) or if it was "more easily accessible to law enforcement or other city officials," then its conclusion would likely change.[271] The Seventh Circuit oddly did not engage with *Whalen* or *Nelson*, two cases that would have naturally supported its conclusions.

Part I's ode to smart meters should have persuaded you that, on balance, the town of Naperville is better off for having them installed. But *Naperville* highlights a fundamental tension in smart meter privacy. There are huge public benefits to having smart meters as a tool for grid management. Utilities need this information for a host of extremely important purposes, and most of the initiatives that utilities want to use the data for will only help consumers. Few would object to their utility being promptly informed that their house is now without power due to a storm, for instance. But there are many other potential uses for this data. What about energy-efficiency studies? Public-awareness campaigns? Identifiable data provided to researchers, or even private for-profit vendors of smart energy solutions? Even if you agree that a warrant should be required for law enforcement access to smart meter data, that still leaves unresolved any number of privacy questions.

This Part showed that obtaining smart meter data from a private utility for law enforcement purposes implicates the Fourth Amendment and should require a warrant. It also showed that a public utility installing a smart meter for non-law enforcement purposes, and therefore collecting the data directly, also implicates the Fourth Amendment. The Fourth Amendment analysis required by *Nelson* and *Whalen* makes clear that non-law enforcement government information gathering will be subjected to a nuanced reasonableness analysis. This requires the kind of detail work that is hard to manage working solely from constitutional first principles. And there is a real danger here of ending up with low constitutional protection against government information collection if there is no statutory protection against private information collection, which can be seen in how the Court's analysis in *Nelson* turned on the practices of private employers. This is an area that could therefore benefit greatly from legislative action to set minimum privacy standards for both

271. *Id.* at 529. The Seventh Circuit's concern with duration and the party collecting the data are similar to concerns raised by both Justice Sonia Sotomayor and Justice Samuel Alito. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *vacated*, 565 U.S. 1189 (2012))); *id.* at 429 (Alito, J., concurring) ("Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.").

governmental and private information collection. Part III therefore moves away from the constitutional analysis and considers legislative solutions to energy privacy. It examines both the solutions already enacted in several states as well as some proposed federal legislation. Ultimately, we set out a model for how energy privacy should be regulated.

III. PROPOSED SOLUTION TO PROTECTING ENERGY DATA

The data collected by smart meters, including information from interconnected devices, provides utilities with insight into when and how energy is being used in short increments of time. As discussed in Part I, that information can be used to increase the efficiency and effectiveness of the current grid and transform it into a smart grid. Better managing how and when energy is produced and used will be key to reducing both carbon emissions and costs.[272] Thus, the information supplied by smart meters can and should be used by utilities to achieve these goals.

Since this information should be collectable, the question then becomes what rules and regulations must be applied to that collection. Here, state and federal legislative action may prove superior to relying on courts. The legislative process is much better suited for the kind of detailed factfinding required to create a unified regulatory scheme. And federal regulation may be particularly helpful in that it would avoid problems of uneven and haphazard local action.[273] Courts, by contrast, are bound by the facts of the cases presented to them and are often unable or unwilling to provide guidance beyond those facts. *Carpenter*, for instance, raised questions about dozens of issues and it may be years before courts give clear answers to any of them.[274]

Further, Fourth Amendment litigation concerns only government action—it does not apply to private companies.[275] One can therefore regulate all law enforcement use of smart meter data via the Fourth Amendment but not all commercial use of it. This could lead to awkward results, with those who happened to live in municipalities with public utilities enjoying privacy protection while those in municipalities with private utilities being left entirely at the mercy of data brokers. As mentioned in Part II, it could also ultimately undermine constitutional privacy protection if energy-usage data is not also protected in the private sphere; courts might be reluctant to impose a warrant requirement for data that can be freely obtained on the open market. A legislative body,

272. Horne et al., *supra* note 51, at 65.

273. *See* Forbush, *supra* note 109, at 375 ("The very real possibility of ratepayer energy consumption data being unevenly regulated by state legislatures and public service commissions demonstrates the need for a baseline privacy standard set at the national level.").

274. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

275. Jackson v. Metro. Edison Co., 419 U.S. 345, 349–50 (1974).

however, can always impose additional safeguards beyond those required by the Constitution and can regulate both private and public entities.

The United States currently does not have a single comprehensive federal law regulating the collection and use of personal data.[276] Instead it has a "patchwork system of federal and state laws . . . that can sometimes overlap, dovetail and contradict one another."[277] At the federal level, for example, banking privacy is regulated by the Gramm-Leach-Bliley Act,[278] educational privacy by the Family Educational Rights and Privacy Act,[279] and health privacy by the Health Insurance Portability and Accountability Act.[280] Sometimes these focused privacy regulations are powerful. The Illinois Biometric Information Privacy Act,[281] for example, has enabled a wave of lawsuits.[282] Yet other times they are comparatively toothless. All three of those federal statutes lack a private right of action.[283]

Due to the depth and breadth of data now collected by electric, gas, and water smart meters, it is time that this domain too receive its own targeted federal regulatory scheme. The question is how best to structure that regime. As will be seen below, we borrow aspects from many other privacy laws. Overall, the regime seeks to empower the Federal Trade Commission (FTC) to regulate the collection of smart meter data, giving it the kind of enforcement authority that it enjoys under the Fair Credit Reporting Act[284] and requiring it to issue the kinds of guidelines that it

276. *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/DJY3-JGSA].

277. Ieuan Jolly, *Data Protection in the United States: Overview*, WESTLAW (2018), https://1.next.westlaw.com/6-502-0467?transitionType=Default&contextData=%28sc.Default %29.

278. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended at 15 U.S.C. § 6803 (2018)).

279. Pub. L. No. 93-380, 88 Stat. 571 (1974) (codified as amended at 20 U.S.C. § 1232g).

280. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 26 U.S.C.).

281. 740 ILL. COMP. STAT. 14/1 (2008).

282. Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, U.C. IRVINE L. REV. 107, 108–09, 113 (2019).

283. George C. Hlavac & Edward J. Easterly, *FERPA Primer: The Basics and Beyond*, NAT'L ASS'N OF COLLEGES & EMPLOYERS (Apr. 1, 2015), https://www.naceweb.org/public-policy-and-legal/legal-issues/ferpa-primer-the-basics-and-beyond/ [https://perma.cc/F7PW-X6HY] ("Courts have routinely held that FERPA does not create a private right of action against the educational institution."); *Can a Patient Sue for a HIPAA Violation?*, HIPAA J. (Nov. 7, 2017), https://www.hipaajournal.com/sue-for-hipaa-violation/ [https://perma.cc/XP88-MNSW]; *The Gramm-Leach-Bliley Act*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/glba/ [https://perma.cc/8AX7-6JFM] ("Enforcement rests solely with federal government agencies, leaving the individual no private right of action.").

284. Pub. L. No. 91-508, 84 Stat. 1114, 1128 (1970) (codified as amended at 15 U.S.C. § 1681–1681x).

did under the Children's Online Privacy Protection Act of 1998.[285] Due to the FTC's current charge to protect consumer data, expanding its responsibility and enforcement power into the area of smart meter data would be the most effective solution at this time.

This Part outlines the major features of that proposed legislation—the Energy Use Privacy Act (EUPA). This Act would explicitly empower the FTC to regulate the use of smart meter data within set guidelines, including addressing when government actors should be able to access smart meter data and when and how it should be shared with private companies. In creating this new regulatory regime, this Article draws inspiration from current statutes in other sectors and proposed statutes that have not yet passed.[286] Further, several states have already started legislating in this area and provide excellent models for the kind of data regime that is vital to protecting consumer privacy.[287] Ultimately, a uniform and consistent regulatory framework for smart meter data and the devices that connect to the meters could enable the United States to achieve smart grid development while also protecting private consumer information.

Before detailing this proposed legislation, it is worth reviewing both a previous federal proposal for energy privacy as well as the FTC's more general role in the privacy space. Though there is no current comprehensive federal legislation protecting energy privacy, the proposed federal Electric Consumer Right to Know Act,[288] sponsored by then-Senators Mark Udall (D-Colo.) and Scott Brown (R-Mass.), would have provided some protection. It stated that "consumers should have the right to control the electric energy usage information of the consumers and the right to privacy for the information when third party aggregators of data are involved in creation, management, or collection of the information."[289] The proposed Act also stated that "consumers should

285. Pub. L. No. 105-277, 112 Stat. 2681-728 (codified as amended at 15 U.S.C. § 6501). Congress has repeatedly outsourced such regulations to the FTC. *See, e.g.*, *id.*

286. For example, "the Gramm-Leach-Bliley Act (GLB) obligates financial institutions to respect the privacy of customers and protect the security and confidentiality of those customers' 'nonpublic personal information' by monitoring their sharing of customer information with third parties." Forbush, *supra* note 109, at 354 (quoting 15 U.S.C. §§ 6801–6809). The Fair Credit Reporting Act requires institutions to prevent the disclosure of private information and issues fines if its requirements are violated. FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS 60, 89–90 (2011).

287. Cassarah Brown, *States Get Smart: Encouraging and Regulating Smart Grid Technologies*, NAT'L CONF. ST. LEGISLATURES (July 2013), http://www.ncsl.org/research/energy/regulating-and-encouraging-smart-grid-technologies.aspx [https://perma.cc/3A5K-6LYP].

288. S. 1029, 112th Cong. (2011).

289. *Id.* § 2(7).

retain the right to the privacy and security of electric energy usage information of the consumers created through usage."[290]

The limitation of this proposed Act is that it was more focused on providing consumers with the right to understand and access their electric-usage information and less on protecting that information from other parties. Though empowering consumers through disclosure is a helpful starting point—and certainly preferable to not providing information to consumers—far more protection is necessary. As an increasingly large body of literature shows, there is great reason to be skeptical of any approach to privacy that relies heavily on people actively seeking out information and making informed choices.[291] Most people do not want to read long privacy policies or actively manage their privacy in the consumer sphere. Also, disclosure will only accomplish so much, especially when, as here, people have limited ability to change utility service providers.

The desire to move beyond disclosure leads to a focus on set rules. As an initial step in establishing these rules, it is essential to identify a single agency to oversee the responsible sharing of smart meter data. Smart meters are likely to interface with a variety of optional consumer smart home products. Were these interfacing products regulated by the FTC (which has evolved into the de facto federal protector of consumer privacy[292]) while the meters themselves were regulated by, say, the Department of Energy, policy could easily grow incoherent. Therefore, localizing the responsibility to govern information sharing in a single entity is preferred. This distinguishes between the immediate use of smart meter data for smart grid management, which should be operated by local utilities, and the use of the data for other purposes, which should be subject to FTC oversight.

Currently, the FTC is the agency most directly involved in the privacy regulation of smart home devices. Under Section 5 of the FTC Act,[293] the

290. *Id.* § 2(6).

291. *See* Florencia Marotta-Wurgler, *Even More Than You Wanted to Know About the Failures of Disclosure*, 11 JERUSALEM REV. LEGAL STUD. 63, 71–72 (2015); Florencia Marotta-Wurgler, *Self-Regulation and Competition in Privacy Policies*, 45 J. LEGAL STUD. S13, S16 (2016) (showing that privacy policies claiming compliance with privacy certifications are often not actually in compliance); Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S 485, 487 (2015); Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1885 (2013); Jedidiah Bracy, *Are Notice and Consent Possible with the Internet of Things?*, IAPP (Nov. 20, 2013), https://iapp.org/news/a/is-notice-and-consent-possible-with-the-internet-of-things/ [https://perma.cc/Q2LD-C6XC]. For a limited defense of notice and choice, see M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1047–50 (2012).

292. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600–06 (2014).

293. Act of Mar. 21, 1938, Pub. L. No. 75-447, 52 Stat. 111, 111 (codified as amended at 15 U.S.C. § 45(a)(1) (2018)).

FTC is charged with preventing companies from engaging in "unfair or deceptive acts or practices in or affecting commerce."[294] This has been the main source of its regulatory authority for enforcing privacy policies and preventing egregious misuses of consumer data.[295] This enforcement, however, largely takes the form of requiring companies to not lie in their privacy policies,[296] and companies may be able to avoid FTC enforcement merely by not making promises about how they will manage private data.[297] Moreover, the FTC's emphasis on regulating companies through their privacy policies is limited in light of "[s]ocial science research reveal[ing] that consumers do not read or understand privacy policies, are heavily influenced by the way choices are framed, and harbor many preexisting assumptions that are incorrect."[298] In this way, the FTC's policies in the smart home-device arena reflect the same problems with notice and choice that were just reviewed.[299]

The FTC's approach to privacy regulation has been criticized on other grounds as well. It has been called overly cautious for failing to meaningfully punish large companies such as Google and Apple when they overstep.[300] Prior to June 2019, the FTC's largest privacy fine was in 2012 for $22.5 million.[301] The subject of the fine, Google, earned $46 billion in revenue that year.[302] And, notably, the FTC could only issue that fine because Google violated a preexisting consent decree—the FTC does not have direct fining authority under Section 5 and must wait for a bad actor to recidivate in violation of an existing judgment to issue a

294. *Id.*

295. Solove & Hartzog, *supra* note 292, at 600–06.

296. *See id.* at 628–31.

297. *See Privacy and Security Enforcement*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement [https://perma.cc/B7X6-WJUW] (laying out FTC enforcement policies). *See also* Public Statement, Dissenting Statement of Commissioner Joshua D. Wright Regarding the Matter of Nomi Technologies, Inc. (Apr. 23, 2015) (expressing concern that the overzealous enforcement of privacy policies might deter transparency).

298. Solove & Hartzog, *supra* note 292, at 667.

299. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 21–22 (2015).

300. Nicholas Confessore & Cecilia Kang, *Facebook Data Scandals Stoke Criticism That a Privacy Watchdog Too Rarely Bites*, N.Y. TIMES (Dec. 30, 2018), https://www.nytimes.com/2018/12/30/technology/facebook-data-privacy-ftc.html [https://perma.cc/58HX-VET7] ("In more than 40 interviews, former and current F.T.C. officials, lawmakers, Capitol Hill staff members, and consumer advocates said that as evidence of abuses has piled up against tech companies, the F.T.C. has been too cautious.").

301. Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented [https://perma.cc/7YPZ-8WHE].

302. *Alphabet Revenue 2006–2019*, MACROTRENDS, https://www.macrotrends.net/stocks/charts/GOOG/alphabet/revenue [https://perma.cc/Z8G4-LCJX].

monetary penalty.[303] Moreover, the FTC has not filed that many privacy complaints. In fact, it only brought 170 between 1997 and 2014.[304] The recent $5 billion fine against Facebook, which covers years of privacy violations, is exceptional.[305] And even the effectiveness of that fine is disputed, as two of the five FTC Commissioners filed dissenting statements calling it inadequate.[306]

In one representative smart home device case, the FTC filed a complaint against TRENDnet for security flaws in its home security cameras.[307] These cameras were supposed to have both public and private modes.[308] The public mode was supposed to be visible to anyone with an appropriate link.[309] The private mode was supposed to be visible only to people with the correct login credentials.[310] Due to a software flaw, even private feeds were publicly viewable and camera IP information even revealed the approximate locations of the video feeds.[311] The FTC alleged that TRENDnet's claims of security constituted false or misleading representations because it "failed to provide reasonable security to prevent unauthorized access to the live feeds from its IP cameras."[312] In short, TRENDnet had promised private feeds and not delivered them. The FTC required TRENDnet to establish a comprehensive security program and provide additional technical and physical safeguards to prevent such a thing from happening again.[313] Notably, it did not fine TRENDnet.[314] It settled a similar case against D-Link on similar terms in July 2019.[315]

As shown in *TRENDnet*, this enforcement is very focused on two kinds of privacy problems. First is the broken promise. A camera or

303. *See* Solove & Hartzog, *supra* note 292, at 605.

304. *Id.* at 600.

305. Cecilia Kang, *F.T.C. Approves Facebook Fine of About $5 Billion*, N.Y. TIMES (July 12, 2019), https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html [https:// perma.cc/WKV9-KQLC].

306. Public Statement, Dissenting Statement of Commissioner Rohit Chopra Regarding the Matter of Facebook, Inc. (July 24, 2019); Public Statement, Dissenting Statement of Commissioner Rebecca Kelly Slaughter Regarding the Matter of *FTC vs. Facebook* (July 24, 2019).

307. Complaint at 4, *In re* TRENDnet, Inc., No. C-4426 (Jan. 16, 2014).

308. *Id.* at 2.

309. *See id.* at 5.

310. *See id.*

311. *Id.* ("[The] compromised live feeds . . . allowed the unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities.").

312. *Id.* at 6.

313. Agreement Containing Consent Order at 4, *In re* TRENDnet, Inc., No. C-4426 (Jan. 16, 2014).

314. *See id.*

315. *See* Lesley Fair, *D-Link Settlement: Internet of Things Depends on Secure Software Development*, FED. TRADE COMMISSION (July 2, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/d-link-settlement-internet-things-depends-secure-software [https://perma.cc/2ZAY-93CA].

network is described as private, but the company fails to deliver on that privacy guarantee. Second is the unauthorized hacker. Information is supposed to be restricted to those with security credentials, but it can be more widely accessed. An FTC staff report on the Internet of Things echoes this emphasis, listing security as its first issue.[316] There is a sense in which this is the bare minimum that the government can ask of a company—do not affirmatively lie and do not leak private information by accident. The much harder question is whether the government should go further. When should *intentional* (as opposed to accidental, hacked, or leaked) sharing of consumer information be limited? That same FTC staff report notably waffled on this issue. The report was summarizing the conclusions of a workshop discussion on privacy in the Internet of Things and the participants appear to have been extremely divided.[317] Some participants were concerned about companies discovering unexpected uses for consumer data, while other participants thought minimizing data collection to prevent such future uses would "chok[e] off potential benefits and innovation."[318]

Consider a third-party energy-monitoring product called Sense. This product works independently of a smart meter; the user must install physical clamps around the main power leads.[319] The device then measures electrical usage several times a second, using the resultant data as inputs for the same kind of device disaggregation described earlier.[320] It is a classic Internet of Things device that just happens to duplicate the functionality of a particularly intelligent smart meter. By default, it is going to be regulated under the same FTC consumer-privacy framework as the cameras in *TRENDnet*. Given that it is going to be within the FTC's purview and will force the FTC to confront all the same data-sharing trade-offs as smart meters, it makes sense to also task the FTC with regulating smart meters themselves.

But even if the FTC chooses not to apply a heightened privacy standard to Internet of Things devices, the lack of choice involved in the utility sphere—people often cannot choose their utility or whether to have a smart meter—shifts the balance in favor of more restrictions. People must actively choose to install Sense whereas they likely will not be able to choose whether to have a smart meter installed. Even if the Internet of Things in general should remain something of a wild west, here there should be greater regulation. We therefore propose legislating additional

316. *See* FED. TRADE COMM'N, *supra* note 299, at 10.

317. *Id.* at 3–4.

318. *See id.* at 21 (alteration in original) (quoting Dan Caprio, McKenna, Long & Aldridge, LLP).

319. *How It Works*, *supra* note 58.

320. *See id.*; *see also supra* notes 98–99 and accompanying text (explaining device disaggregation).

authority for the FTC, allowing it to serve a more proactive role than its baseline Section 5 authority permits. Specifically, the FTC should be required to issue regulations for the protection of consumer data—rather than the advice and recommendations that it puts out in the data-security context—and to enforce those regulations with monetary fines. In this way, EUPA should mirror the enforcement authority given to the FTC under the Fair Credit Reporting Act.[321]

This role of the FTC is the most important part of the proposal. The basic idea of protecting consumer privacy in this domain, at some level, has been around for a while. Some of the principles we promote were reflected in the Voluntary Code of Conduct proposed by the Department of Energy in 2015, for instance.[322] But the very first word in the title of that document reveals its most fundamental problem: "voluntary." Energy-consumption data pierces the walls of the home, invading what are otherwise the most protected spaces in daily lives. Industry self-regulation and voluntary compliance are insufficient here.

A. *Use of Smart Meter Data by the Utilities*

Many of the benefits of smart meters for grid management involve the use of smart meter data by the utilities themselves. It is the utility, after all, that needs to know about localized power outages, to calibrate production to meet demand, and to selectively deactivate portions of the grid in emergencies. To realize these benefits, smart meter information does not need to be shared beyond the utility and its chosen (and carefully monitored) subcontractors. There should, therefore, be a sharp distinction between use of this information by the utility for internal purposes, which should be presumptively allowed without restriction, and use by any other actor. Since the utility is the entity that naturally collects smart meter data and has the most use for it, it makes the most sense for the utility, whether it be publicly or privately owned, to be the primary custodian of smart meter data. Keeping this data housed within utilities may also reassure consumers, who are more likely to trust their utilities than third parties.[323]

The privacy protections of smart meter data available to consumers should not depend on the type of utility serving their area. For the most

---

321. Pub. L. No. 91-508, 84 Stat. 1114, 1128 (1970) (codified as amended at 15 U.S.C. § 1681–1681x (2012)).

322. U.S. DEP'T OF ENERGY, VOLUNTARY CODE OF CONDUCT (VCC): FINAL CONCEPTS AND PRINCIPLES 1 (2015), https://www.energy.gov/sites/prod/files/2015/01/f19/VCC%20Concepts%20and%20Principles%202015_01_08%20FINAL.pdf [https://perma.cc/8M54-UVC7].

323. Chien-fei Chen et al., *Between the Technology Acceptance Model and Sustainable Energy Technology Acceptance Model: Investigating Smart Meter Acceptance in the United States*, 25 ENERGY RES. & SOC. SCI. 93, 101 (2017) (noting that the participants of the Amazon Mechanical Turk survey "generally trusted their utilities, but were fairly concerned with unauthorized third parties' misuse of [smart meter] data or personal information").

part, consumers are unable to switch between utility providers; thus, leaving consumers exposed to varying levels of data protection based on the public, private, or ambiguously mixed character of the utility is problematic. Instead, a uniform set of protections should be established for all consumers.

In the context of a publicly owned utility, questions may be raised as to what governmental entity owns the smart meter data. In that case, ownership should be limited to the utility itself and not a larger governing body, such as the city or township.[324] The goal of this new regulatory scheme is to limit the access to the smart meter data while providing utilities with the ability to manage the smart grid. Allowing the smart meter data to be housed by a governmental entity other than the public utility risks exposure of this private data to a wider group of people, potentially including law enforcement.

As the constitutional information-privacy cases like *Nelson* and *Whalen* illustrate,[325] courts should distinguish between different government uses of information when weighing privacy rights. Utilities are properly positioned to use this data both for the benefit of grid management and to protect consumers. The proposed regulatory scheme would not only establish that utilities are owners of the smart meter data, but it would also establish guidelines and regulations around when commercial entities and law enforcement agencies can access and utilize the data. Since these entities are seeking to access the data for different purposes—market development for one[326] and in aid of investigations for the other[327]—different guidelines must apply to them.

---

324. EISEN ET AL., *supra* note 25, at 71–72 (noting that public power systems can include local, municipal, state, and regional utilities, which can range in size from tiny municipal distribution companies to giant systems such as the Los Angeles Department of Water and Power; some are regulated by state public utility commissions and others are regulated by local governments or are self-regulated); *What is Public Power?*, PUB. POWER FOR YOUR COMMUNITY, https://www.publicpower.org/system/files/documents/municipalization-what_is_public_power.pdf [https://perma.cc/PU4Z-P6VT] ("Most public power utilities are owned by cities and towns, but many are owned by counties, public utility districts, and even states.").

325. *See supra* Section II.D.

326. Forbush, *supra* note 109, at 367 ("[P]otential commercial uses for smart meter data include use by '[r]etailers of appliances, extended warranties, or repair services [who] may want [smart meter] data . . . to provide advertising . . . before an appliance fails,' and '[i]nsurers [who] may want to look for evidence of unauthorized conduct . . . .'" (alterations in original) (quoting Mark F. Foley, *The Dangers of Meter Data (Part I)*, SMARTGRIDNEWS.COM (June 2, 2008), http://www.smartgridnews.com/artman/publish/Technologies_Metering_News/The_Dangers_of_Meter_Data_Part_1-446.html)).

327. United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1114 (9th Cir. 2012) ("A DEA agent filed an affidavit in the district court stating that the subpoenaed [electricity-consumption] records were relevant to determine whether individuals at three residences were involved in the manufacture and distribution of controlled substances."); McLean, *supra* note 64,

B. *Law Enforcement Access*

Though law enforcement agencies have a strong and legitimate interest in detecting illegal activities occurring in a home and verifying a suspect's claims about what occurred in a home, the new regulatory regime must incorporate the baseline understanding that consumers have an expectation of privacy in the smart meter data generated from their homes. As discussed in Part II, consumers are not necessarily consenting to the installation of smart meters or freely sharing this data with the utilities—these are required aspects of modern-day life. Moreover, law enforcement must not be able to utilize the business-records exception to access smart meter data records collected by a private utility.[328]

This is a substantial change from current practice. There has been a long "history of voluntary utility compliance with government requests to share personal consumer usage information."[329] Though a few states have statutes protecting consumer utility data, even these privacy-protective states often allow utilities to respond to requests by law enforcement if they have subpoena or other court order rather than insisting on a warrant.[330] In light of cases like *Kyllo* and *Carpenter*, however, the warrantless provision of smart meter data to law enforcement agencies is overly intrusive. The records of the utilities are simply too revealing and go back too far to allow for sharing without legal process. Law enforcement agencies should have to demonstrate probable cause and argue for the need to access such data before an independent arbiter (that is, "get a warrant") instead of meeting the lower standard required for court orders or subpoenas.

Though a warrant requirement will undoubtedly slow criminal investigations, it will not unduly frustrate the investigative process.

---

at 885 ("Smart meter data present a potential new tool for law enforcement to investigate a broad set of crimes and even track people's whereabouts. Law enforcement could use smart meter data as either direct or circumstantial evidence for any number of crimes."); Affidavit of Probable Cause to Obtain An Arrest Warrant, *supra* note 3 (demonstrating that another example of this occurred in a recent case where a police department in Arkansas was provided the data from a smart water meter by the local utility without a warrant to aid it in the investigation of a murder) ("As previously mentioned, at least 140 gallons of water was used at James' residence in the two hour period between 0100-0300 hours. Upon reviewing all water usage information, since October 2013 at James' residence, this excessive amount of water usage between 0100 and 0300 hours had never before occurred.").

328. *Contra Golden Valley*, 689 F.3d at 1116–17 (holding that consumers lacked a reasonable expectation of privacy in energy-consumption records because they had "no possessory or ownership interest" in the records held by a utility company (quoting United States v. Cormier, 220 F.3d 1103, 1108 (9th Cir. 2000)).

329. McLean, *supra* note 64, at 886.

330. *See, e.g.*, OKLA. STAT. tit. 17, § 710.6 (2019) ("Pursuant to a warrant, subpoena duces tecum, or other court order."); COLO. CODE REGS. § 723-3:3027(b) (2019) ("[T]his includes responses to requests of the Commission, warrants, subpoenas, [or] courts orders . . . .").

Recall that smart meter data is in the custody of the utility. Consumers-cum-criminal suspects do not have the ability to edit or delete their data. Smart meter data is also neither a weapon that suspects can seize nor a bomb that must be quickly located and disarmed. In short, this data can wait.

We can imagine a set of law enforcement uses that might be ill-suited for the warrant process. Smart meter data could be useful, for instance, in determining if a house is presently occupied in advance of a raid or an arrest, or as part of a manhunt. But we are aware of no cases in which it has been used in that fashion. So, though we are open to persuasion that there are cases in which a narrow exigency exception must be added to the statute, we do not believe we need to craft one quite yet. If one is necessary, the Wiretap Act provides a suitable model for *ex post* approval under special circumstances and Congress could easily borrow the language from that statute for this one.[331]

More controversially, EUPA should go further than imposing a warrant requirement by borrowing portions of the superwarrant requirements from the Wiretap Act.[332] These additional requirements are burdensome and are part of the Wiretap Act because of the uniquely sensitive information contained in real-time communications. But they are justified in this context as well. The home is a special place; allowing the government to see through its very walls is precisely the kind of technological development that has so upset the Court in cases like *Kyllo*. A judge should therefore need to find probable cause that particular information concerning the offense will be obtained from the smart meter data requested. Further, the court must find that alternatives to accessing the smart meter data were attempted and failed, or "reasonably appear to be unlikely to succeed if tried or to be too dangerous."[333] To prevent this from becoming a routine request, only government officials of a certain level should be able to apply for a warrant to access the data.[334] Finally, to protect against unnecessary governmental access, the updated provision should minimize the amount of information that can be produced in response to the warrant—limited to very specific time periods to avoid sweeping in data beyond the scope of the initial order.[335]

In crafting these additional restrictions, we seek to restrict two possible types of bulk data collection. First, the police should not be able to request smart meter data for an entire residential district to determine

331. 18 U.S.C. § 2518(7) (2018).

332. *See* Paul Ohm, *The Investigative Dynamics of the Use of Malware by Law Enforcement*, 26 WM. & MARY BILL RTS. J. 303, 329–31 (2017) (discussing de facto superwarrant protections, particularly in relation to the Wiretap Act).

333. *See, e.g.*, 18 U.S.C. § 2518(1)(c) (imposing a similar requirement for wiretaps).

334. *See, e.g.*, *id.* § 2516(1) (imposing a similar requirement for wiretaps).

335. *See, e.g.*, *id.* § 2518(5) (imposing a similar requirement for wiretaps).

who was home at a given time. Second, the police should not be able to engage in, or require utilities to engage in, data mining based on an energy-use suspect profile.[336] In each case, there is an easy argument that the information is relevant to potential investigations and thus might satisfy a subpoena requirement. The additional restrictions would make it much harder to justify these sorts of requests.

C. *Private Access*

Government actors are not the only parties that are interested in accessing smart meter data. Many private companies, including those working to develop energy-efficiency or renewable-energy programs for utility customers, would like access to develop their products, enhance their algorithms, and target their potential clients.[337] Private companies will also be involved in the development of the smart grid, especially in creating appliances and software applications for smart home energy-management systems. To encourage innovation and new developments in this area, these companies need to be allowed to create products that will interact with smart meters—it is only through automation and interconnectivity that the true potential of the smart grid will be realized.

But the risk associated with smart grid development is that the extremely private information will be gathered from the home—the place where privacy is the most important. Marketers, among other private companies, will want to tap into this data to find out helpful information about the household to target certain products to it.[338] Targeted advertising of an individual or a household represents an area of huge interest. For example, prior work in this area suggested that "they could use energy consumption data to identify heavy energy users, cross-reference that data with households that have not applied for a new furnace permit in twenty years, and target those residents for furnace replacement programs."[339]Additionally, insurance companies are interested in accessing home smart meter data for underwriting purposes.[340] These companies are outside of the consumer–utility relationship and therefore require additional restrictions on what they can access.

---

336. Generally, this applies to marijuana-growing operations.

337. Andrew Bartholomew, Note, *The Smart Grid in Massachusetts: A Proposal for a Consumer Data Privacy Policy*, 43 B.C. ENVTL. AFF. L. REV. 79, 92 (2016) ("If these third parties were permitted to acquire consumer usage information directly from the utilities, it might create an avenue through which commercial efficiency operations could identify potential customers and market their services accordingly.").

338. Forbush, *supra* note 109, at 367 (noting that the potential commercial uses for smart meter data include appliance retailers, repair-service companies, and insurance-coverage companies).

339. Klass & Wilson, *supra* note 12, at 1100.

340. Forbush, *supra* note 109, at 367.

One study has indicated,

> [t]rust concerns might also arise from perceived loss of control, especially the control over [smart meter] data, so utilities enterprise managers should allow customers to retain some level of control and . . . combat misperceptions that [smart meter]s are designed to control residents' energy consumption at any time and monitor them like "big brother."[341]

To have more control over their smart meter data, consumers need to be made aware of exactly the kind of data that a company is able to collect from their homes and how the data is being used and provided some mechanism for control of that data. Moreover, consumers should be able to decide whether to share their data with private companies and, after sharing it, limit what their data may be used for. An important goal of any legislation in this area should be to prevent the creation and sale of electronic dossiers of consumers' home lives as catalogued by their smart meters and connected smart devices. And, due to consumers' limited time and attention, an effective regulatory regime cannot rely solely on boilerplate grants of customer consent. Protecting privacy will require more than a one-time check box.

For commercial entities, EUPA should include provisions that provide consumers with more information and power to protect their private data. As a model for this kind of regulation, consider the example of the California Consumer Privacy Act.[342] In 2018, California passed the most progressive privacy law in the United States, which provides consumers with several new rights related to their personal data.[343] The Act includes the right to know what personal information a business has collected and the right to opt out of allowing a business to sell personal information to third parties, and it requires third-party data disclosures to consumers.[344]

Other states also have statutory privacy protections that do not allow utilities to share monthly consumer data without the customer's written or electronic consent.[345] Ohio goes further by requiring that utilities also include a statement highlighting customers' right of refusal to have their data released.[346] Texas prohibits an electric utility from "selling, sharing, or disclosing information generated, provided, or otherwise collected

341. Chien-fei Chen at al., *supra* note 323, at 101.

342. CAL. CIV. CODE § 1798.100 (West 2019).

343. Jolly, *supra* note 277, at 5.

344. CIV. § 1798.100.

345. *See Data Access*, AM. COUNCIL FOR ENERGY-EFFICIENT ECON., https://database.aceee.org/state/data-access [https://perma.cc/5TST-JLL3].

346. *See* OHIO ADMIN. CODE 4901:1-10-05(J) (2019).

from an advanced metering system."[347] But the Texas public utility commission allows an electric utility to share information with an affiliated corporation or other third-party entity "*if* the information is to be used only for the purpose of providing electric utility service to the customer or other customer-approved services."[348] Similarly in Colorado, utilities are only authorized to utilize customer smart meter data "exclusively in furtherance of predefined smart grid goals."[349] Congress can look to these provisions when deciding which consumer protections it wants to include in EUPA. At a minimum, consumers should be notified when utilities seek to share their smart meter data and should receive information about whether they are able to decline to participate.

One possibility that does not appear to have been explored is the use of the utility as a communication portal between third parties and utility customers. Imagine that an energy-efficiency company believes that its product can save money for customers with a given energy profile. One approach would be to allow the utility to sell a list of such customers to the company without consumer consent. This is problematic from a privacy perspective for obvious reasons. Another approach is to allow consumers to opt into third-party marketing. This is better from a privacy perspective but runs into serious scope-of-consent issues—it would be a challenge to appropriately calibrate how much information should go from utility to company or to sensibly decide how many companies should get the data, and one could easily imagine most consumers finding the choice confusing. A third possibility would be to have the utility serve as a matchmaker. It could host an energy-efficiency portal (as many utilities do) and populate it with offers from energy companies that the utility's own data suggest are good matches for the consumer. The consumer could then decide whether to reach out to the companies. This would, in a way, be nothing more than an expansion of energy-efficiency programs, such as the Home Energy Assessment program, offered by many utilities.[350] This would also provide consumers with a single point of contact if they wish to assert, or waive, privacy protections.

The above describes the challenge of marketing—how to connect consumer to company to allow for socially beneficial transactions—but does not as directly address product development. How can companies safely be given enough information to enable them to create new energy-efficient solutions? Here it may be beneficial to borrow from another federal privacy statute, the Health Insurance Portability and

347. TEX. UTIL. CODE ANN. § 39.107(k) (West 2019).

348. *Id.* (emphasis added).

349. McLean, *supra* note 64, at 898.

350. *See, e.g.*, *Home Energy Assessment*, COMED, https://www.comed.com/WaysToSave/ForYourHome/Pages/SingleFamily.aspx [https://perma.cc/MUN7-ECTM].

Accountability Act (HIPAA).[351] Both medical and energy research benefit greatly from the sharing of individual information, yet there are also great privacy risks in both contexts. The HIPAA solution to this dilemma is to have two possible channels for research use of medical information.[352] The first is to allow free use of de-identified information.[353] In the energy domain this could cover many uses. Though location-based characteristics are relevant to energy analysis, the biggest of those is weather, and weather is notoriously large. One does not need block-level granularity to track the effect of temperature increases on air-conditioning costs. The FTC could do exactly what the U.S. Department of Health and Human Services did in the HIPAA context: develop guidelines for what constitutes sufficiently de-identified data in this domain and allow utilities to distribute exactly that much information.[354] The FTC should also have companies obtaining this de-identified data agree to certain use restrictions, particularly a restriction on efforts to re-identify consumers or to link the smart meter data to individually identifiable datasets.

HIPAA also allows for the use of individually identifiable health information in research under tight restrictions.[355] In general, this information can only be obtained for specific planned research studies (rather than general "may be useful later" studies) that have been reviewed by an ethics board.[356] Furthermore, the information must be carefully protected, and the affected patient must give consent.[357] These requirements seem ill-suited for the kind of big-data approaches that energy-efficiency companies wish to employ. The de-identified path is therefore likely to be better suited for most energy projects. As described in the next Section, many local utilities are already implementing this kind of information sharing using their own standards for anonymization.

---

351. Though we disagree with Alexandra Klass and Elizabeth Wilson on many points, we think they are correct to use HIPAA as a model for making energy consumption data available for research purposes.

352. *See* 45 C.F.R. § 164.502(c)-(d) (2019).

353. *See id.* § 164.502(d).

354. *See id.* § 164.514(a)–(c) (outlining the guidelines for what constitutes sufficiently de-identified data).

355. *See id.* § 164.502(c). *See generally* DEP'T OF HEALTH & HUMAN SERVS., PROTECTING PERSONAL HEALTH INFORMATION IN RESEARCH: UNDERSTANDING THE HIPAA PRIVACY RULE (2004), https://privacyruleandresearch.nih.gov/pdf/HIPAA_Booklet_4-14-2003.pdf [https://perma.cc/KV38-U99T] (describing broadly the rules and regulations that apply when using identifiable health information in research).

356. *See* DEP'T OF HEALTH & HUMAN SERVS., *supra* note 355, at 11.

357. *Id.* at 11–12.

D. *Incorporating Smart Grid Development Goals into EUPA*

A final consideration that must be addressed within EUPA itself is the recognition of the importance of smart meter data to the development of the smart grid. As discussed in Part I, utilities have a real need for this data and sharing smart grid data with each other and other entities in the energy industry would go far in assisting with the smart grid. Much of this data can and should be anonymized before sharing to better protect consumers' information. Fortunately, there are several different models currently in existence for sharing this data that can serve as an example for Congress.

Many utilities are starting to share anonymized energy-usage data to encourage the continued development of the smart grid. For example, Chicago's utility, ComEd, now shares anonymized usage data with commercial entities looking to develop new products, academics and researchers using the data for energy-related scholarship, and companies looking to develop new technology for the home.[358] Illinois law prohibits ComEd and other utilities "from sharing customers' billing and usage data without authorization, but it allows more freedom to share 'generic information.'"[359] In Vermont, utilities are required to share "town-scaled aggregate data" with the statewide energy-efficiency program administrator to demonstrate which "communities have achieved the greatest saving through efficiency, and also how much the need for new electricity generation has been reduced."[360] These examples demonstrate how anonymized, aggregated data can help energy-efficiency providers and smart grid developers with more information about energy usage. Ultimately, this information could help both utilities and other companies optimize the smart grid and reduce energy consumption.

In addition to voluntarily anonymizing customer data, many utilities also participate in the Green Button Initiative, which "fosters the development, compliance, and adoption of the global Green Button electricity-, natural gas-, and water-usage data-sharing standard" and enables consumers to share their energy-usage data without any personal

358. *See* David J. Unger, *Illinois Regulators Approve Utility Plan to Share Anonymous Energy Usage Data*, ENERGY NEWS NETWORK (Feb. 21, 2017), https://energynews.us/2017/02/21/midwest/illinois-regulators-approve-utility-plan-to-share-anonymous-energy-usage-data/ [https://perma.cc/C7AV-XKT6] (noting that ComEd's "Anonymous Data Service removes any personal information—including names, addresses and electric account numbers—that might identify individual users").

359. *Id.*

360. AM. COUNCIL FOR AN ENERGY-EFFICIENT ECON., BEST PRACTICES FOR WORKING WITH UTILITIES TO IMPROVE ACCESS TO ENERGY USAGE DATA 9 (2014).

information attached to it.[361] The Initiative helps customers protect their private data while also encouraging them to share their energy-usage data with interested third parties to better understand how they are consuming energy.[362] The Green Button Alliance, which includes utility members who are a part of the Green Button Initiative, joined the DataGuard Energy Data Partnership Program, which "is a voluntary program that provides high-level principles around the treatment, retention and disposal of customer data."[363] This program can also serve as a guide to Congress when writing the necessary provisions of EUPA. It is vital that EUPA encourage and enable the sharing of energy-usage information to help with the continued development of the smart grid.

A final consideration for the protection of consumers' smart meter data is understanding the risk of other devices connecting to the smart meter and potentially also recording the smart meter data. While the risk presented by the growth of the Internet of Things and interconnected devices in the home is outside the scope of this Article, Congress should consider building in additional protections for devices that specifically overlap with the smart meters in smart homes. For example, EUPA could require a warrant for law enforcement to obtain all information collected by the covered devices to ensure that all private power information is afforded a consistent level of protection. EUPA could be written broadly to be more inclusive in regard to the kind of devices that may connect to a smart meter; "the exact technology that collects the information is not the crucial point, but rather the *nature* of the information collected will trigger the application of [the] statute."[364]

While this solution is not a silver bullet and there will be continued problems with both public and private entities improperly accessing smart meter data, it is the most straightforward solution to start protecting smart meter data today. Technology is progressing so fast that both the courts and Congress have not been able to keep up with it. Time is of the

361. *Green Button Alliance Launches Green Button Connect My Data (CMD) Certification Program for Electricity, Natural Gas, and Water Utilities*, GREEN BUTTON ALLIANCE (Sept. 5, 2018, 9:00 AM), https://www.prnewswire.com/news-releases/green-button-alliance-launches-green-button-connect-my-data-cmd-certification-program-for-electricity-natural-gas-and-water-utilities-300706792.html [https://perma.cc/JM64-V6FU]; *see also Green Button for My Home*, GREEN BUTTON DATA, http://www.greenbuttondata.org/residential.html [https://perma.cc/CY4A-9SS8] (explaining how the program operates and how consumers can sign up).

362. Unger, *supra* note 358.

363. *Smart Energy Consumer Collaborative and Green Button Alliance Become Inaugural Members of DataGuard Energy Data Privacy Partnership Program*, GREEN BUTTON ALLIANCE (June 27, 2018), https://www.greenbuttonalliance.org/smart-energy-consumer-collaborative-and-green-button-alliance-become-inaugural-members-of-dataguard-energy-data-privacy-partnership-program [https://perma.cc/T7XM-YQUF].

364. Bianchini, *supra* note 103, at 26 (arguing for an amendment to the Electronic Communications Privacy Act with a fourth statute to encompass noncommunicative intimate information collected by digital assistants).

essence—Congress needs to act now to ensure that consumers' intimate data from the home is adequately protected. EUPA provides at least one path forward for allowing the necessary access to important smart grid data while also protecting consumers' privacy in the home.

CONCLUSION

The development of the smart grid creates many benefits for energy efficiency, environmental protection, and grid stability. The challenge is whether society may allow the full exploitation of those benefits while still protecting consumer privacy. Since society is currently at the precipice of huge technological changes both in the home and in the smart grid, now is the time to build in additional protections for consumers and their homes.

Writing his dissent in *Olmstead v. United States*[365] in 1928, Justice Louis Brandeis recognized the risk that technology and the progression of science posed to the people of the United States. He noted:

> "[I]n the application of a constitution, our contemplation cannot be only of what has been but of what may be." The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[366]

It is fair to say that society may have reached the point that Justice Brandeis was alluding to. Accessing smart meter data provides the government with encyclopedic insight into occurrences and activities within the home—perhaps the last sacred place recognized by the Fourth Amendment. Yet current Fourth Amendment protections likely do not go far enough in protecting smart meter data from improper use. Therefore, Congress must step in to provide additional safeguards against this kind of collection of information from the home. The proposed solution—EUPA—will not protect everything that occurs within the home, but it prevents both the government and commercial entities from capitalizing on this new required technology. The Act would require a warrant before law enforcement may access smart meter data. It would also require consumer knowledge and consent before their private data may be shared with commercial entities. And it would place the regulation and oversight

365. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

366. *Id.* at 474 (Brandeis, J., dissenting).

of this intimate data within the purview of one federal agency that can track and monitor the utilization of smart meter data.

Finally, the efficient and effective use of smart meters is key to combating climate change. Instead of getting in the way of utilities sharing and utilizing this necessary information, EUPA would recognize the importance of anonymizing and aggregating community energy-usage data. It is integral that utilities have this data to increase the efficiency of the grid as a whole and to help decarbonize the electricity sector, but the government must implement safeguards to protect consumers and the intimacies of the home. EUPA provides a way to encourage smart grid development while also protecting consumers' data privacy. And due to the continued advancement of technology in this area, no more time can be spared in creating a regulatory framework that addresses these issues. Smart meters should be optimized along with the development of the smart grid, but their optimization should not come at the cost of consumer privacy.