How Smart Is Too Smart?: How Privacy Concerns Threaten Modern Energy Infrastructure

ABSTRACT

Smart meters are integral to the health of our electric grid and are critical to a reliable, affordable, and efficient energy economy. Yet, collection of smart meter data is raising privacy concerns that are inspiring pockets of resistance to smart meter installation around the country. The fact that these data, like many other kinds of personal information, can and often do flow to the government should not prevent their collection and use. It is critical for environmental and energy regulators to have access to this data to maximize the potential of our energy system. On the state level, several legislatures and Public Utility Commissions (PUCs) have enacted a variety of rules and regulations designed to balance privacy concerns with smart grid goals. But by looking beyond trade-offs between privacy and smart meter installation, this Note recognizes an opportunity to protect reasonable expectations of privacy without hampering the ability of the smart grid to reach its full potential. This can be accomplished by shifting the conversation from regulation of smart meter installation *to regulation of smart data* distribution.

TABLE OF CONTENTS

I. INTRODUCTION

To celebrate the new millennium, the National Academy of Engineering identified the most important engineering achievements of the twentieth century. The Internet ranked thirteenth on this list, and "highways" were eleventh.[1] Sitting at the top of the list was something most Americans encounter each day with the flick of a switch or the click of a button. Electrification, as made possible by the grid, was far and away "the most significant engineering achievement of the 20th century."[2]

However, we have taken this marvelous machine for granted for far too long. As a result, our overburdened grid is struggling to keep up with our increasingly large, complex energy demands and is desperately in need of an upgrade. In 2009, President Obama announced the largest single grid modernization investment in US history.[3] The Smart Grid Investment Grant (SGIG) program seeks to accelerate the transformation of the nation's electric grid by deploying smart grid technologies and infrastructure. Under the American Recovery and Reinvestment Act of 2009 ("Recovery Act"), the US Department of Energy (DOE) and the electricity industry jointly invested over $7.8 billion in ninety-nine cost-shared SGIG projects.[4]

1. *See generally* GEORGE CONSTABLE & BOB SOMERVILLE, A CENTURY OF INNOVATION: TWENTY ENGINEERING ACHIEVEMENTS THAT TRANSFORMED OUR LIVES (Joseph Henry Press, 2003).

2. *Id.*

3. *See* The Energy Independence and Security Act of 2007 § 1301, 42 U.S.C. § 17381 (2007).

4. *See* U.S. DEP'T OF ENERGY, OFFICE OF ELEC. DELIVERY & ENERGY DELIVERY, SMART GRID INVESTMENT GRANT PROGRAM PROGRESS REPORT 7 (July 2012), https://www.smartgrid.gov/

With funds provided by the Recovery Act, thirty-two municipalities, including Los Angeles, Baltimore, and New Orleans, are deploying smart grid technologies and systems.[5] According to the US Federal Energy Regulatory Commission (FERC), more than 45.8 million smart meters were installed across the nation by July 2013, covering more than a third of all US electrical customers.[6] More smart meters are being installed every day.[7]

The term "smart grid" encompasses a vast network of controls, communications, automation, and new technology working together to make the energy sector greener, more efficient, more reliable, and more secure. But for most people, it is symbolized by one thing: the smart meter. Installed in place of traditional, mechanical meters, digital smart meters do more than simply record the number of kilowatt-hours used by a customer each month. They break down energy usage into smaller discrete periods of time and open a channel of communication between the customer and the utility company. This information helps households cut energy costs and increases reliability by providing utilities with more information about how much electricity is being used throughout their service areas.

However, privacy concerns are inspiring powerful pockets of resistance to smart meter installation around the country, making it increasingly difficult for states and municipalities to reap the benefits of this much-needed technology. Utility workers in Pennsylvania are calling widespread smart meter installation "a plot by Obama to spy on us."[8] Echoing similar concerns, the city of Ojai, California, declared a moratorium on smart meter installation in May 2012.[9] In Illinois, an outspoken citizen group sued for an injunction to halt smart meter installations on Fourth Amendment grounds.[10] In Texas, one woman

---

sites/default/files/doc/files/sgig-progress-report-final-submitted-07-16-12.pdf [https://perma.cc/HG3M-LM3R].

5. *See* U.S. DEP'T OF ENERGY, OFFICE OF ELEC. DELIVERY & ENERGY DELIVERY, MUNICIPAL UTILITIES' INVESTMENT IN SMART GRID TECHNOLOGIES IMPROVES SERVICES AND LOWERS COSTS 1 (Oct. 2014), http://energy.gov/sites/prod/files/2014/10/f18/SG-UtilityInvestment-Oct2014.pdf [https://perma.cc/9PNH-TMU3].

6. *See* FERC, Assessment of Demand Response and Advanced Metering, FERC Staff Report, 3 (Dec. 2014), http://www.ferc.gov/legal/staff-reports/2014/demand-response.pdf [https://perma.cc/439T-A4FT].

7. *Id.*

8. Christina Nunez, *Who's Watching? Privacy Concerns Persist as Smart Meters Roll Out,* NAT'L GEOGRAPHIC NEWS (Dec. 14, 2012), http://news.nationalgeographic.com/news/energy/2012/12/121212-smart-meter-privacy/ [https://perma.cc/85QP-FYH9].

9. *See* Ojai, Cal., Ordinance No. 823, § 1 (May 29, 2012).

10. *See* Naperville Smart Meter Awareness v. City of Naperville, 69 F. Supp. 3d 830 (N.D. Ill. 2014).

even pulled a gun on a utility employee trying to install a smart meter on her property.[11]

Though smart meters are not, in fact, a domestic espionage scheme, they do raise important questions: If households are communicating with the power grid, what exactly will be revealed? Perhaps more importantly, who will be listening?

This Note proceeds in five Parts. Part II weighs the revolutionary potential and associated privacy concerns of the smart grid. Part III examines the privacy protections in place to protect personal smart meter data. Part IV analyzes state approaches to improving the energy grid without sacrificing individual privacy. Part V argues for a reframing of the privacy debate and proposes federal legislation, modeled after Colorado's regulatory framework as the optimal means of balancing privacy and energy concerns. Part VI concludes.

II. THE SMART GRID: TWENTY-FIRST CENTURY ELECTRICITY DISTRIBUTION

Smart meters are integral to the health of our current electric grid and are critical to a reliable, affordable, and efficient energy economy. However, smart meter technology raises important privacy concerns, as it can be used to reveal personal information about life within a home to government actors, often without the homeowner's explicit consent.

A. Smart Grid: Solution to a Broken System

The United States' energy grid was designed more than a century ago. As the country's demand for energy continues to increase dramatically in both quantity and complexity, the current grid is desperately in need of an upgrade.[12] The existing energy infrastructure has proven embarrassingly inadequate in the face of extreme weather events, threats of cyber attacks, and the need to

11. *See* Charlie Wells, *Houston Woman Thelma Taormina Pulls Gun on Electric Company Worker for Trying to Install 'Smart Meter'*, N.Y. DAILY NEWS (July 19, 2012, 6:25 PM), http://www.nydailynews.com/news/national/houston-woman-thelma-taormina-pulls-gun-electric-company-worker-install-smart-meter-article-1.1118051 [https://perma.cc/Y6VY-U3GR].

12. The American Society of Civil Engineers recently gave US energy infrastructure a D+ grade, citing the grid's advanced age as a key concern. Am. Soc'y of Civil Eng'rs, 2013 Report Card for America's Infrastructure 1 (2013), http://www.infrastructurereportcard.org/a/documents/Energy.pdf [https://perma.cc/5BRB-Y27P]. Our current electric grid was conceived at a time when homes had only small energy demands, such as a few light bulbs and a radio, and much of our generation, transmission, and distribution facilities date back as far as the 1880s. *Id*.

revolutionize our energy consumption to combat climate change.[13] The "smart grid" uses digital age technology to profoundly change the electric power grid in much the same way that business, education, and entertainment have changed with the advent of the Internet and other transformative technology.[14] Smart technology can be used to update our ailing electric grid making it more reliable, secure, and efficient.

The existing electricity grid is increasingly unreliable. This is correlated with the increasing regularity of power outages in the United States: there have been five massive blackouts over the past forty years—three of which happened in the past decade.[15] These outages have broader implications than simply waiting for the lights to come on: plant production stops, perishable food spoils, traffic lights go dark, and credit card transactions are rendered inoperable.[16] Outages and reliability issues are estimated to cost American businesses more than $100 billion each year.[17] The increase in blackouts and brownouts is due, in large part, to slow response times of mechanical switches, a lack of automated analytics, and a lack of situational awareness on the part of grid operators.[18] Currently, utilities only learn of a power outage when a customer calls to report it.[19] The smart grid enables utilities to identify outages, their cause, and the customers affected as soon as they occur.[20] This allows utilities to quickly reroute electricity to customers and reduce the impact of an outage.[21] Advanced smart grid technology also allows utilities to monitor the health of the grid proactively, allowing them to repair pending faults in advance and avoid outages.[22]

The current electric grid is also vulnerable to cyber attack. Technologically, electric utilities are about a decade behind financial

---

13. *See id.*

14. *See* Joel B. Eisen, *Smart Regulation and Federalism for the Smart Grid*, 37 HARV. ENVTL. L. REV. 1, 7 (2013).

15. *See* Sudeen G. Kelly, *Effectively Transforming our Electric Delivery System to a Smart Grid: Hearing Before the Subcomm. on Energy & Environment of the Comm. on Science & Technology*, 111th Cong. (2010), http://www.ferc.gov/EventCalendar/Files/20090723104313-Kelly%20Smart%20Grid%20Testimony.pdf [https://perma.cc/TNA2-V5H7].

16. The Northeast blackout of 2003 resulted in a $6 billion economic loss to the region. *See id.*

17. Litos Strategic Comm'n, *The Smart Grid: An Introduction*, U.S. DEP'T. OF ENERGY 6 (2008).

18. Samuel J. Harvey, *Smart Meters, Smarter Regulation: Balancing Privacy and Innovation in the Electric Grid*, 61 UCLA L. REV. 2068, 2072–73 (2014).

19. *See id.*

20. *See id.*

21. *See id.*

22. *See id.* at 2073; Stephanie M. Stern, *Smart-Grid: Technology and the Psychology of Environmental Behavior Change*, 86 CHI.-KENT L. REV. 139, 144 (2011).

and telecommunications industries when it comes to protecting against cyber hackers. Utilities across the country, and around the world, have seen a significant increase in deliberate attacks that could throw thousands of customers into the dark.[23] In April 2009, The Wall Street Journal reported that cyber spies had infiltrated the US electric grid and left behind software that could be used to disrupt the system.[24] According to the Journal, the hackers, stemming from China, Russia, and other nations, were on a phishing expedition to map out our electric system.[25] The interdependencies of various grid components present the risk of a cascading series of failures that could bring our nation's banking, communications, traffic, and security systems to a halt. While some worry that as the number of digital touch points increases, potential vulnerability to cyber attacks likewise increases. The smart grid can actually keep the electrical system more secure because it senses trouble earlier, sends in cyber troops to protect data, and diverts power around trouble spots.[26]

Moreover, smart grid technology increases efficiency by decreasing both the amount of electricity consumed and the amount lost in transition. The US Energy Information Administration (EIA) predicts that the deployment of a national smart grid system could reduce electricity demand by as much as 38 to 48 percent.[27] Smart meters provide real-time demand information, enabling utilities to produce only as much energy as needed, thereby minimizing surplus, as energy is lost unless consumed upon generation. This information also reduces peak load provisions, decreasing the need for "peaker plants," the oldest, dirtiest, most dangerous plants that only come online when demand is highest.[28] Moreover, consumer access to smart meter data enables consumers to make smarter, more efficient, and more cost-effective energy consumption choices.

In short, upgrading to a smart grid benefits consumers, utilities, businesses, and society as a whole. It achieves environmental goals at lower costs than the traditional grid, enables

23. Eric Niiler, *Energy Grid: Safe From Cyber Attack?*, DISCOVERY NEWSLETTER (May 9, 2012, 3:00 AM), http://news.discovery.com/tech/apps/smart-grid-cyber-attacks-110901.htm [https://perma.cc/TM9P-9GHA].

24. Siobhan Gorman, *Electricity Grid in U.S. Penetrated By Spies*, WALL ST. J. (Apr. 8, 2009, 11:59 PM), http://www.wsj.com/articles/SB123914805204099085 [https://perma.cc/UGP6-HYHQ].

25. *Id.* Phishing is typically characterized by an attempt to acquire sensitive information, such as usernames and passwords, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

26. A small attack happening in one place will be easier to isolate, and other resources can be brought to bear, minimizing the damage that the bad guys are intending. *See id.*

27. *See* Stern, *supra* note 22, at 145.

28. *See id.* at 143–44.

us to respond more quickly to natural and man-made outages, and operates more efficiently and reliably.

B. So Smart It's Scary: Potential for Government Overreach

As previously stated, smart meters generate individual privacy concerns because consumption data can be used to reveal personal details about life within a home. While traditional analog meters record monthly energy consumption as a single lump sum figure, smart meters collect between 750 and 3,000 distinct time-stamped data points per month.[29] Typical smart meters record energy usage every fifteen minutes, while advanced versions may shrink this window to as few as six seconds or even permit measurement in real time.[30] Individual appliances increasingly have unique energy consumption patterns. For example, a refrigerator draws power in a different way than a television, a respirator, or a marijuana grow light.[31] As a result, there is a concern that these data may be aggregated over time and analyzed to reveal personal information including medical conditions, illicit habits, or other private details about a person's home life.[32]

Consequently, utility customers and privacy advocates have expressed concerns about law enforcement access to smart meter data.[33] 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. They have the potential to be used to identify marijuana grow houses, sweat shops, brothels, or to detect violations of housing ordinances or zoning regulations. The data can also be used to uncover fraud, substantiate or disprove an alibi, or suggest whether a home's residents conspired to commit a crime.[34]

---

29. Jack I. Lerner & Deirdre K. Mulligan, *Taking the Long View of the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3, 3 (2008).

30. *See* Sonia K. McNeil, Note, *Privacy and the Modern Grid*, 25 HARV. J.L. & TECH. 199, 204 (2011).

31. *See* Jian Liang et al., *Load Signature Study—Part I: Basic Concept, Structure, and Methodology*, 25 IEEE TRANSACTIONS ON POWER DELIVERY 551, 551 (2010).

32. *See, e.g.*, McNeil, *supra* note 30, at 204–05.

33. *See, e.g.*, Ojai, Cal., Ordinance No. 823, § 1 (May 29, 2012); Naperville Smart Meter Awareness v. City of Naperville, 69 F. Supp. 3d 830, 836 (N.D. Ill. 2014); Nunez, *supra* note 8; Wells, *supra* note 11.

34. *See* Cheryl Dancey Balough, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161, 171 (2011) (suggesting that smart meter data could be used to frustrate a reimbursement claim for a medical device you are not actually using, to show you were home on a certain night, or that your home security system was disarmed at the time of a burglary).

These concerns are not unfounded. In the United States, there is a history of voluntary utility compliance with government requests to share personal consumer usage information.[35] In some areas of the country, law enforcement already uses energy consumption data to investigate potential illegal activities. In Texas, a police detective used individual energy data obtained from a public utility company to identify residential marijuana growing operations.[36] Similarly, in California, law enforcement officers obtained a warrant to search a family home for evidence of marijuana production based on an unusually high electric bill.[37] In both cases, the alleged data mining focused on above-average overall electricity consumption.[38] Smart meter data could allow for much more focused investigations, as consumption could potentially be tracked by appliance or time of day.

The increasing amount of personal information readily available to the government poses significant problems with far-reaching social effects. Inadequately constrained government information gathering can result in the "slow creep toward a totalitarian state."[39] This makes individuals particularly vulnerable to government misuse of personal information during times of crisis.[40] There is a concern that insufficient privacy protections chill "democratic activities and interfer[e] with individual self determination."[41] Concerns such as these engender public outcry and community bans on smart meter technology.[42]

However, the fact that smart meter data, like many other kinds of personal information, can—and often do—flow to the government should not necessarily prevent their collection and use.[43] It is critical for environmental and energy regulators to have access to these data to maximize the potential of our energy system. For present purposes, what is important is that potential abuses are mitigated where

35. *See id.* at 172 (discussing telephone companies' willingness to share consumers' personal phone records with law enforcement after the 9/11 attacks).

36. *See* Jordan Smith, *APD Pot-Hunters Are Data-Mining at AE*, AUSTIN CHRONICLE (Nov. 16, 2007), http://www.austinchronicle.com/news/2007-11-16/561535/ [https://perma.cc/B4DJ-7K9E].

37. *See* Balough, *supra* note 34, at 171.

38. *See id.* at 172; Smith, *supra* note 36.

39. *See* Katrina Fischer Kuh, *Personal Environmental Information: The Promise and Perils of the Emerging Capacity to Identify Individual Environmental Harms*, 65 VAND. L. REV. 1565, 1600–01 (2012).

40. *See id.*

41. *See id.*

42. *See, e.g.*, Ojai, Cal., Ordinance No. 823, § 1 (May 29, 2012); Naperville Smart Meter Awareness v. City of Naperville, 69 F. Supp. 3d 830, 836 (N.D. Ill. 2014); Nunez, *supra* note 8; Wells, *supra* note 11.

43. *See* Nunez, *supra* note 8.

possible and otherwise accounted for when balancing privacy concerns with societal goals.

C. It Takes a Village: Smart Meter Installation as a Collective Action Problem

Smart grid technologies have a public good dimension due to the societal benefits—like efficiency, reliability, and security—that can be achieved and the inability to exclude electricity users from enjoying these benefits. Privacy concerns create incentives to free ride on smart meter data provided by neighbors. Energy consumers can free ride by opting out of smart meter installation and choosing to retain their traditional analog meters while continuing to enjoy the benefits of a smart grid.

Like flu shots, smart meters give off positive externalities. The more people who install them, the more efficient the smart grid becomes. This results in fewer blackouts, more reliable electricity, a greener planet, and economic savings for both consumers and utilities. Similarly, the costs imposed by failing to adopt smart meters are largely public. Free riders impose costs on the system, both in the form of imperfect data collection and, more concretely, in the form of a meter reader, who comes to their home each month to maintain and monitor the traditional meter. Inability to exclude certain consumers from the modern grid means those who opt out still benefit from the data shared by friends and neighbors without having to bear any of the risks of sharing their own data.

Due to concerns about privacy, all over the country individuals, communities, and even entire states are opting out, imposing enormous costs on our energy system while continuing to share in the benefits the smart grid provides.

III. LEGAL PROTECTION: SMART METER DATA AND THE FOURTH AMENDMENT

In order to help develop new regulatory regimes to address these privacy concerns, we should look to existing rules and legal structures governing access to similar data. The Fourth Amendment provides the primary means of balancing individual privacy with the government's legitimate need to access information. The Fourth Amendment sets limits on law enforcement's investigatory powers,

including its ability to obtain data.[44] The Supreme Court interprets Fourth Amendment privacy protections in terms of "reasonable expectations";[45] however, the application of reasonable expectations of privacy to emerging technology has proven exceedingly difficult.[46]

Importantly, the Supreme Court has consistently found that individuals can have no reasonable expectation of privacy for information willingly conveyed to third parties.[47] This reasoning, termed the "third-party doctrine," has been extended by the Court to include information customers provide to businesses, including utilities.[48] In contrast, however, the Supreme Court has repeatedly affirmed the importance of the home as the location afforded the most privacy under the Fourth Amendment.[49]

A. A Man's Home Is His Castle

The Fourth Amendment prohibits the warrantless use of technology to view inside a home. In 2001, the Supreme Court addressed this issue in *Kyllo v. United States*.[50] In *Kyllo*, a government agent viewed a private residence using a thermal imaging device.[51] The images revealed interior temperatures consistent with the presence of marijuana grow lights.[52] While a marijuana grow house was indeed present, the Court found thermal imaging to be an impermissible warrantless search. To the Court, the use of imaging

---

44. *See* U.S. CONST. amend. IV (providing that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated").

45. *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). In *Katz*, a defendant was convicted of transmitting wagering information by telephone in violation of a federal statute. *See id.* at 348. At trial, the government introduced evidence of telephone conversations overheard by FBI agents who had attached an electronic listening and recording device to the outside of a telephone booth without obtaining a warrant. *See id.* The Supreme Court held the evidence was illegally obtained, explaining, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *See id.* at 351. Consequently, after *Katz*, the Fourth Amendment protects objects, activities, and statements from warrantless search where (1) a person exhibits a subjective expectation of privacy and (2) that expectation is one that society finds objectively reasonable. *See id.* at 348, 351; *see also id.* at 361 (Harlan, J., concurring).

46. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 505 (2007).

47. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

48. *See, e.g.*, United States v. McIntyre, 646 F.3d 1107, 1111–12 (8th Cir. 2011) (holding that there is no reasonable expectation of privacy protected by the Fourth Amendment in residential electricity usage records).

49. Kyllo v. United States, 533 U.S. 27, 40 (2001).

50. *See generally id.*

51. *Id.* at 29–30.

52. *Id.* at 30.

technology was, for Fourth Amendment purposes, equivalent to entering Kyllo's home.[53] The Court justified its holding by reasoning that such technology could disclose intimate details about personal activities, including "at what hour each night the lady of the house takes her daily sauna and bath."[54] Justice Scalia opined that the Fourth Amendment draws a firm line at the entrance to the house.[55]

However, in the majority opinion, Justice Scalia also specified that "intrusion into a constitutionally protected area, constitutes a search—at least where . . . the technology in question is not in general public use."[56] This caveat suggests that if a technology for seeing inside a house is in "general public use," then that technology might invalidate societal willingness to accept the individual's expectation of privacy as reasonable.

B. Third-Party Doctrine

Traditionally, courts have applied a two-part inquiry to decide whether data shared with a third party receive Fourth Amendment protection. First, the court asks if the individual actually exhibited an expectation of privacy. If so, the next question is whether the subjective expectation of privacy is one that society recognizes as reasonable. For information shared with a third party, the Court's answer to the second question has uniformly been "no." [57]

The Supreme Court has "consistently held that a person has no legitimate expectation of privacy regarding information that he voluntarily turns over to third parties."[58] The foundational Supreme Court challenge to the practice on Fourth Amendment grounds is found in *On Lee v. United States*.[59] This case established that law enforcement does not violate the Fourth Amendment by using third parties to obtain information without first seeking a warrant.[60] According to the Court, the Fourth Amendment was only designed to protect reasonable expectations, not "a wrongdoer's misplaced belief

53. *See id.* at 40.

54. *Id.* at 38.

55. *Id.* at 40 (the line protecting privacy of the home "must be not only firm but also bright").

56. *Id.* at 34.

57. *See McNeil*, *supra* note 30, at 213 (citing Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

58. *Smith*, 442 U.S. at 743–44.

59. *See generally* On Lee v. United States, 343 U.S. 747 (1952).

60. *See id.*

that a person to whom he voluntarily confides his wrongdoing will not reveal it."[61]

This misplaced belief rationale was subsequently extended to business records. In *United States v. Miller,* the Court refused to suppress bank records that corroborated a defendant's intent to defraud the government of taxes owed on an illegal moonshine operation.[62] In revealing his affairs to the bank, the Court held that the defendant assumed the risk that his information would be shared with law enforcement.[63]

Using the same reasoning, lower courts have held that there is no reasonable expectation of privacy in the data contained in electric utility records.[64] Courts reason that because there is no privacy interest in records kept in the course of a business, under *Miller,* individuals cannot challenge law enforcement's acquisition of various types of information such as bank records, credit card statements, and cell phone records.[65] Thus, under the third-party doctrine, consumers seemingly have no reasonable expectation of privacy in the smart meter data contained in electric utility records either.

However, academics are increasingly advocating for a reframing of third-party doctrine as a doctrine of consent.[66] These advocates recognize that the third-party doctrine makes two assumptions: first, that there was a choice to disclose information to a third party; and second, that the consent to disclose information to a third party remains viable even if the third party permits the government, to whom no consent was given, to access the data. Framed instead as a doctrine of consent, the second question becomes "did the person's choice to disclose information to a third party constitute consent to a search by law enforcement?"[67] Viewed in this light, the answer may not always be yes.

---

61. Hoffa v. United States, 385 U.S. 293, 302 (1966).

62. *See* United States v. Miller, 425 U.S. 435, 437–43 (1976).

63. *See id.* at 442, 447 (reaffirming that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"); *see, e.g., Smith*, 442 U.S. at 744–45; Couch v. United States, 409 U.S. 322, 335–36 (1973); United States v. White, 401 U.S. 745, 752 (1971); *Hoffa*, 385 U.S. at 302; Lopez v. United States, 373 U.S. 427 (1963).

64. *See, e.g.*, United States v. Hamilton, 434 F. Supp. 2d 974, 980 (D. Or. 2006); Samson v. State, 919 P.2d 171, 173 (Alaska Ct. App. 1996); People v. Dunkin, 888 P.2d 305, 308 (Colo. App. 1994); Booker v. Dominion Va. Power, No. 3:09CV759, 2010 WL 1848474, at *9–10 (E.D. Va. May 7, 2010).

65. *See Miller*, 425 U.S. at 442.

66. *See* McNeil, *supra* note 30, at 216.

67. *See id.*

C. The Naperville *Holding*

Courts have repeatedly held that citizens have no reasonable expectation of privacy in the aggregate measurements of their electrical usage.[68] In September 2014, the District Court for the Northern District of Illinois explicitly expanded this holding to include smart meter data.[69]

In 2012, a public utility serving the small city of Naperville, Illinois, began replacing customers' analog electricity meters with smart meters as part of a local program called the Naperville Smart Grid Initiative ("Initiative"), an SGIG program.[70] The Initiative did not include an avenue for customers to keep their traditional analog meters, requiring all electricity customers to have a smart meter installed so the city's electric utility and residents could maximize benefits from the Initiative.[71] The newly installed smart meters increased the frequency of meter readings from once a month to once every fifteen minutes.[72] These data were used by the city to increase cost efficiency, conserve energy, and optimize the performance of the local energy grid.[73]

The plaintiff, Naperville Smart Meter Awareness (NSMA), is an Illinois not-for-profit corporation whose stated mission is to "educate, engage and empower families, friends and neighbors to advocate for a fiscally responsible and safe utility meter solution in Naperville, Illinois."[74] NSMA alleged that smart meters present privacy risks because a home's smart meter data history reveals "intimate details about residents' personal lives and living habits."[75] Thus, NSMA claimed that Naperville's collection of detailed smart meter data constituted an unreasonable search under the Fourth Amendment and sought an injunction.[76]

In September 2014, the federal district court dismissed NSMA's Fourth Amendment claim. The court held that there is no

---

68. *See, e.g.*, United States v. McIntyre, 646 F.3d 1107, 1111–13 (8th Cir. 2011) (holding that there is no reasonable expectation of privacy protected by the Fourth Amendment in residential electricity usage records).

69. *See generally* Naperville Smart Meter Awareness v. City of Naperville, 69 F. Supp. 3d 830, 841 (N.D. Ill. 2014).

70. *See id.* at 835.

71. Naperville Smart Grid Initiative, Question/Response Inventory 6 (Mar. 25, 2013), http://www.naperville.il.us/emplibrary/Smart_Grid/NSGIQuestionResponseInventory.pdf [https://perma.cc/5D36-7BP9].

72. *See id.*

73. *See id* at 6, 8, 22–23.

74. *Id.* at 4.

75. *Id.* at 5.

76. *See id.* at 15–16.

reasonable expectation of privacy protected by the Fourth Amendment in residential electricity usage records, even in smart meter data.[77] The court reasoned that smart meters do not convey any information in which residents have a reasonable expectation of privacy.[78] According to the court, even if a graph displaying a home's total power usage for one day shows a peak in usage around 7:00 PM, a person inspecting the data might infer that someone was home at that time.[79] However, that same inference could also be reasonably made by any member of the public walking by the residence who notices a car in the driveway or lights in the window.[80] Thus, the data provided by smart meters are not information that can reasonably be expected to remain private.[81] While this was only a district court decision, it is the only decision on smart meters to date. Thus, although it is not binding on other courts, it is likely indicative of how other courts will view smart meter data under the Fourth Amendment.

IV. WALKING THE TIGHT-ROPE: BALANCING PRIVACY NEEDS AND SMART GRID GOALS

Every day, our energy grid is becoming more reliant on smart meter data.[82] Better information regarding household energy usage is improving meaningful efforts by utilities and regulators to improve the efficiency and reliability of our energy system.[83] However, the ultimate success or failure of the smart grid hinges on customer acceptance.[84] While the majority of meters installed by utilities receive little customer resistance, the demands of a small, but very vocal, coalition of customers have had a significant impact on regulatory policy. Despite the tremendous need for smart meters,

77. *See* Naperville Smart Meter Awareness v. City of Naperville, 69 F. Supp. 3d 830, 841 (N.D. Ill. 2014).

78. *See id.* ("Because NSMA has not alleged that the City is collecting any information that is more detailed than aggregate usage measurements, or that is otherwise entitled to protection under the Fourth Amendment, NSMA has failed to state a claim for unreasonable search and seizure.").

79. *See id*.

80. *See id.*

81. *See id.*

82. *See* Smart Meter Deployments Continue to Rise, U.S. ENERGY INFO. ADMIN. (Nov. 1, 2012), http://www.eia.gov/todayinenergy/detail.cfm?id=8590 [https://perma.cc/82N6-LXZV].

83. *See supra* Section II.A.

84. *See* Beth Karlin, *Public Acceptance of Smart Meters: Integrating Psychology and Practice*, *in* ACEEE SUMMER STUDY ON ENERGY EFFICIENCY IN BUILDINGS: FUELING OUR FUTURE WITH EFFICIENCY 1 (2012), http://www.aceee.org/files/proceedings/2012/data/papers/0193-000243.pdf [https://perma.cc/9G2X-8HV7] ("Public acceptance of utility programs and initiatives is vital for efficient deployment. Consumer complaints, protests, and lawsuits, can significantly impede progress and cost utilities, cities, and taxpayers money.").

grassroots opposition has spread across the United States, leaving a trail of opt-out policies in its wake.[85] In order to maximize the potential of this new technology, regulators must balance these privacy concerns with smart grid goals.

A. Failure of the Fourth

Academics have suggested that the sanctity of the home in Fourth Amendment jurisprudence, coupled with the level of detailed information about the interior of a home revealed by smart meters, may be sufficient to overcome the third-party doctrine.[86] If law enforcement were to collect smart meter data directly, it could arguably be considered a search within the meaning of the Fourth Amendment. Like thermal imaging in *Kyllo*, smart meters may be used to reveal personal information about the interior of a home and the lives of its residents.[87] In fact, smart meter data can even be used to determine "at what hour each night the lady of the house takes her daily sauna and bath."[88]

Others suggest that if the third-party doctrine is viewed as a doctrine of consent, Fourth Amendment protections could be applied to some forms of smart meter data.[89] For many categories of information, sharing is clearly a deliberate choice. For smart meter data, however, this "choice" is harder to find when customers are left without the option of retaining their traditional analog meter. Living without basic utility services, such as electricity or water, is akin to keeping one's savings under a mattress, rather than in a bank.[90] While it may be possible, it is not within the realm of the normal. In states with extreme temperatures, living without basic utility services may actually be impossible at times.[91] In this context, the choice to share information with a third party is the choice to turn on the furnace, the lights, the refrigerator, or the respirator. It is, in other words, not very much of a choice at all.

In practice, however, smart meter data is probably not protected by the Fourth Amendment. While the Supreme Court has

85. *See, e.g.*, Ojai, Cal., Ordinance No. 823, § 1 (May 29, 2012); *Naperville*, 69 F. Supp. 3d at 841; Nunez, *supra* note 8; Wells, *supra* note 11.

86. Brandon J. Murrill et al., Cong. Research Serv., R42338, *Smart Meter Data: Privacy and Cybersecurity* 3 (2012), http://www.fas.org/sgp/crs/misc/R42338.pdf [https://perma.cc/424F-2V7Y]; *see* Harvey, *supra* note 18, at 2068.

87. Kyllo v. United States, 533 U.S. 27, 29–30 (2001).

88. *Id.* at 40.

89. *See* McNeil, *supra* note 30, at 216.

90. *See id.*

91. For this reason, "cold weather rules" limit a utility's ability to cut off service during some months, even to a non-paying customer in some states. *See id.* at 217.

not explicitly applied the third-party doctrine in this instance, lower court decisions have repeatedly extended the doctrine to utility records, strongly implying that the doctrine extends to smart meter data.[92] Moreover, smart meter data may not be protected even if the third-party doctrine did not apply. Justice Scalia's dicta in *Kyllo* seemingly states that if technology for seeing inside a house is in "general public use," then its use does not constitute a violation of the Fourth Amendment.[93] As smart meters become more prevalent, already occupying more than a quarter of American households,[94] it is foreseeable that society could find the expectation unreasonable that one's electricity-consuming activities inside the home would remain private.

Ultimately, the *Naperville* decision appears to be the last nail in the coffin for any hope that the Fourth Amendment is sufficient to protect individual smart meter data.[95] The court directly addressed the granular nature of smart meter data and the personal details that can be inferred from such a detailed data set and still found it insufficient to warrant a reasonable expectation of privacy.[96] As a result, Congress must extend protection beyond that provided by the Fourth Amendment by creating legislation and regulations designed to better address the privacy concerns presented by smart meter data while maintaining clear procedures for law enforcement to follow in order to gain access to customer information.

B. Laboratories of Experimentation

On the state level, several legislatures and Public Utility Commissions (PUCs) have enacted a variety of rules and regulations designed to balance these competing objectives. New Hampshire's smart meter deployment policy prohibits utilities from installing smart meters without the express written consent of the customer. Vermont, meanwhile, encourages statewide smart meter adoption, but allows customers to opt out at any time. California also encourages statewide adoption of smart meters, but charges a monthly fee to

92. *See, e.g.*, United States v. Hamilton, 434 F. Supp. 2d 974, 980 (D. Or. 2006); Samson v. State, 919 P.2d 171, 173 (Alaska Ct. App. 1996); People v. Dunkin, 888 P.2d 305, 308 (Colo. App. 1994); Booker v. Dominion Va. Power, No. CIV.A. 3:09CV759, 2010 WL 1848474, at *5 (E.D. Va. May 7, 2010).

93. *Kyllo*, 533 U.S. at 40.

94. *See Smart Meter Deployments Continue to Rise*, U.S. ENERGY INFO. ADMIN.: TODAY IN ENERGY (Nov. 1, 2012), http://www.eia.gov/todayinenergy/detail.cfm?id=8590 [https://perma.cc/QF5R-AS2S].

95. *See* Naperville Smart Meter Awareness v. City of Naperville, 69 F. Supp. 3d 830, 841 (N.D. Ill. 2014).

96. *See id.*

customers who decide to opt out. While these state opt-out policies serve to protect citizens from real and imagined threats to their privacy, they also serve to undermine the ultimate goals of the Recovery Act and thwart the implementation of the much-needed smart grid.

1. New Hampshire's Consent Model

Implemented in 2012, New Hampshire has one of the most restrictive approaches to smart meter deployment. The New Hampshire approach is very effective at preserving the privacy of its citizens by choosing to frame smart meters as the exception, instead of the rule. Rather than making smart meters the default and allowing residents an opportunity to opt out, New Hampshire requires residents to opt in to its smart meter program. In New Hampshire, no electric utility can install a smart meter without the express written consent of the customer.[97] The state actively discourages installation by requiring electric utilities to inform homeowners that smart meter installation is optional and prohibiting the provision of reduced rates or incentives of any kind for customers who opt to install smart meters,[98] even though smart meters save utilities money by reducing the need for meter men and increasing grid reliability.

As a result of these restrictive policies, the bulk of New Hampshire residents do not have to worry about the government getting ahold of detailed smart meter data without the resident's knowledge or consent. However, the state fails to protect the privacy of residents who elect to have smart meters installed. Due to the stringency of the notice and consent requirements, New Hampshire residents who consent to smart meter installation have likely waived their reasonable expectation of privacy under even the modern iteration of the third-party doctrine because they knowingly consented to share their personal data with their utility company.

In addition, by deterring smart meter installation, New Hampshire prevents its residents from reaping the full benefits of the smart grid.[99] Here, the externalities imposed by failing to adopt smart meters are largely public. While individual privacy is protected, the associated costs of an aging grid are borne equally by those who choose to adopt smart meters and those who do not. By discouraging

97. *See* N.H. REV. STAT. ANN. § 374:62 II(a) (LexisNexis 2012) ("No electric utility that sells or provides electricity within the state of New Hampshire shall install a smart meter gateway device on or in a person's home or business without written consent of the person or persons who own the home or business.").

98. *Id.* § 374:62 II(b)(2).

99. For a discussion of the benefits of the smart grid, see *supra* Section II.

smart meter installation in New Hampshire, the state is unduly burdening residents who consent to installation as well as neighboring northeastern states who share both energy infrastructure and environmental impacts.

In sum, the New Hampshire model provides strong privacy protections for many of its citizens, but at a high cost to both its residents and its neighbors.

2. Vermont's Voluntary Opt-Out Program

Vermont is a perfect foil of New Hampshire—geographically, politically, and in terms of its smart meter policy. In Vermont, smart meters are treated as the norm, rather than the exception. Predictably, the result is a much higher level of smart meter adoption than seen in New Hampshire.[100] Consequently, all residents reap the benefits of the smart grid, even those who chose not to have a smart meter installed.

The Vermont Energy Act of 2012 specifies that utility companies transitioning to smart meters must: (1) provide prior written notice to customers indicating that the meter will use radio or other wireless means for two-way communication with the utility, (2) offer a free opt-out option at the time of installation, and (3) allow customers to request removal of a previously installed smart meter for any reason without incurring any charge for removal.[101]

While the state has made a concerted effort to improve its electric grid, like New Hampshire, it has not placed much emphasis on protecting the privacy of its residents who share their smart meter data with their utilities. The Vermont approach likely waives all Fourth Amendment protection. Those with smart meters likely have no reasonable expectation of privacy, as the technology is in general public use in the state, and they are informed annually that they are sharing their data with a third party. Given the notice requirement, consumers likely also consent to share their data with the government under this policy.

Nonetheless, the state does protect the privacy of those who express concerns by mandating an easy opt-out option.[102] Customers may choose not to have smart meters installed at no additional cost.[103] Thus, customers and communities concerned about their privacy have

100. *See* H. Russell Frisby Jr. et al., *Report of the Demand-Side Resources & Smart Grid Committee*, 34 ENERGY L.J. 373, 386 (2013) ("Florida, Texas, Vermont, and the West lead the nation with over 30% advanced metering penetration based on 2012 data.").

101. *See* VT. STAT. ANN. tit. 30, § 2811 (2012).

102. *See id.*

103. *See id.*

a form of recourse. Moreover, the statute permits entire communities to opt out, as seen in Ojai, California.[104]

While this freedom is intended to provide a refuge for those worried about government access to personal data, it is also a useful tool for vocal dissenters to impose community-wide opt outs on entire towns or regions, which can have devastating effects on the proliferation of the smart grid. The Vermont model's lack of privacy protection for smart meter data and ease of opt-out procedures create a recipe for debilitating customer resistance to installation by facilitating free riding. Inability to exclude certain consumers from the modern grid means those who opt out still benefit from the data shared by friends and neighbors without bearing any of the risks.[105]

3. California's Price of Privacy Model

Due in large part to the pressing energy crisis, California has a particularly aggressive plan for smart grid adoption. Like Vermont, California makes smart meter installation the norm. However, California goes two steps further: (1) customers who choose to opt out of the smart meter program are charged a monthly fee,[106] and (2) local governments may not collectively opt out of smart meter programs on behalf of residents in their jurisdictions.[107] The result is almost universal adoption and one of the most successful smart grid programs in the country.[108]

By imposing a fee on those who opt out, California attempts to force would-be free riders to internalize the costs they impose on the system. In 2014, the costs of opting out were updated to reflect the

---

104. *See supra* note 9 and accompanying text; Ojai, Cal., Ordinance No. 823, § 1 (May 29, 2012); *id.*

105. Again, these free riders impose costs on the system, both in the form of imperfect data collection and, more concretely, in the form of a meter reader who has to come to their homes each month to maintain and monitor the traditional meter.

106. Decision Modifying Decision 08-09-039 and Adopting an Opt-Out Program for S. Cal. Edison Co.'s Edison Smartconnect Program, Decision No. D12-04-018 (Cal. P.U.C. Apr. 19, 2012); Decision Modifying Decision 07-04-043 and Adopting an Opt-Out Program for San Diego Gas & Elec. Co., Decision No. D12-04-019 (Cal. P.U.C. Apr. 19, 2012); Decision Modifying Pac. Gas and Elec. Co.'s Smartmeter Program to Include an Opt-Out Option, Decision No. D12-02-014 (Cal. P.U.C. Feb. 1, 2012). Customers participating in the opt-out option are assessed an initial fee of $75 and a monthly charge of $10 thereafter; however, low-income customers are eligible for a reduced rate. *Id.*

107. *See* Application of Pacific Gas and Electric Co. for Approval of Modifications to its Smart MeterTM Program and Increased Revenue Requirements to Recover the Costs of the Modifications (U39M), 2014 Cal. PUC Lexis 637, 4 (Cal. PUC Dec. 18, 2014); Decision Modifying Decision 07-04-043 and Adopting an Opt-Out Program for San Diego Gas & Elec. Co., No. D11-03-015, at 17 (Cal. P.U.C. Apr. 19, 2012).

108. Frisby, *supra* note 100.

actual costs borne by the system.[109] These costs include customer operations, metering, and information technology. However, they do not take into account the more abstract costs to the smart grid like imperfect data or increased inefficiency.[110] Nonetheless, after reviewing their findings, the California PUC still found that the imposition of costs associated with the opt-out program on opt-out customers would result in almost doubling their utility bills.[111] In an attempt to balance the appropriate allocation of costs with the need to set fees at a level that does not unreasonably deter customers from electing the opt-out option, the California PUC instituted a cap on fees imposed on opt-out customers and spread the rest of the costs evenly among all California households.[112]

Like the Vermont approach, this model has been very successful in maximizing smart grid potential and mitigating the impact of free riders. However, it still leaves its residents vulnerable to invasions of privacy. Not only are smart meter data not protected by the state, the California approach likely waives all Fourth Amendment protection. People with smart meters likely have no reasonable expectation of privacy because the technology is in general use, they are informed annually that they are sharing their data with a third party, and they have an opportunity to opt out—all of which likely amounts to consent. As a result, there is a sense of dissatisfaction among residents, although dissenters have very few means of mobilizing resistance.[113]

4. Colorado: Controlled Distribution Model

The Colorado model is unique because it regulates distribution of smart meter data, instead of smart meter installation. In Colorado, utilities are authorized to use customer data exclusively in furtherance of predefined smart grid goals.[114] Otherwise, utilities may not disclose customer data to third parties, including government agents, without the customer's written consent.[115] This ensures that

109. California electric utilities estimate the total opt-out program costs over $60 million per year. *See* U39M, 2014 Cal. PUC LEXIS 637 at 5, 8, 53.

110. *See id.* at 53.

111. *See id.* at 57.

112. *See id.*

113. *CA Local Governments On Board*, STOP SMART METERS! (Feb. 27, 2015), http://stopsmartmeters.org/how-you-can-stop-smart-meters/sample-letter-to-local-government/ca-local-governments-on-board/ [https://perma.cc/6UCN-36S3] (listing fifty-seven local governments in California that are opposed to the mandatory smart meter program).

114. 4 COLO. CODE REGS. § 723-3:3029 (LexisNexis 2016).

115. *Id.* § 723-3:3030.

customer-specific data are used exclusively for purposes that align with consumers' reasonable expectations.

The Colorado PUC also calibrates protection measures to the level of risk posed by different types of data.[116] Utilities can share aggregated data with third parties as long as no individual customer can be identified from the aggregated amount.[117] To ensure individual smart meter data are sufficiently aggregated, Colorado requires at least fifteen customers to be included in each group and specifies that no single customer can account for more than 15 percent of that group.[118]

The Colorado policy is laudable because it protects tiered reasonable expectations of privacy without sacrificing smart grid potential. Like in California and Vermont, smart meter installation is the norm. But, the Colorado model is unique because the state protects consumers' reasonable expectations of privacy regardless of whether they opt to have smart meters installed or not. Because government access to the data is highly regulated, citizens are less concerned about the potential for government overreach and less likely to opt out as individuals or as a community. With these distribution protections in place, privacy concerns should be mitigated for many customers, resulting in widespread smart meter adoption and ushering our grid into the twenty-first century without sacrificing consumer privacy.

These different models provide a helpful framework through which to analyze how best to achieve both privacy and regulatory goals. Comparatively, the New Hampshire model is the most restrictive. It provides strong privacy protections for its citizens at the expense of modernization of the electric grid. In Vermont, smart meters are treated as the norm, but residents are allowed to opt out at no additional cost, resulting in a much higher level of smart meter adoption.[119] California also makes smart meter adoption the default, but imposes a fee on those who opt out in an attempt to force those who do to bear the costs of their decisions. Finally, the Colorado model is unique because it regulates distribution of smart meter data, rather than installation. Each of these states provides an insight into the strengths and weaknesses of different approaches, which are helpful in identifying the best model for states and the nation as a whole going forward.

---

116. *See generally* 4 COLO. CODE REGS. § 723-3 (LexisNexis 2016).

117. *See* 4 COLO. CODE REGS. § 723-3:3031(a) (LexisNexis 2016).

118. *See id.*

119. *See* Frisby, *supra* note 100, at 386 ("Florida, Texas, Vermont, and the West lead the nation with over 30% advanced metering penetration based on 2012 data.").

V. REFRAMING THE ISSUE

Government access to smart meter data is critical to effective regulation of our energy system. It is imperative to facilitate some government access for reliability, efficiency, and security purposes. Yet, unfettered access to smart meter data seems unlikely and ill advised. It opens the door for government overreach and invasion of privacy, to say nothing of citizen discontent and resistance. In states like New Hampshire, opportunities for the smart grid to flourish are frustrated by the adoption of privacy policies developed without recognition of the need to preserve or facilitate such access. Meanwhile, if no or inadequate restrictions on government access are in place, privacy concerns inspire a backlash that precludes smart grid proliferation.[120]

The third-party doctrine most likely eliminates Fourth Amendment protections for an individual's smart meter data.[121] This lack of protection has prompted many fearful utility customers to balk at smart meter installation, delaying or derailing smart grid progress. The time has come for federal regulation.

A. A Job for Congress

In lieu of constitutional protection, congressional legislation is the best way to protect privacy and maximize smart grid potential. Congress has already recognized the smart grid as a national priority, as seen by its heavy investment through the American Recovery and Reinvestment Act of 2009.[122] Moreover, the health and security of the electrical system directly impact national security, the national economy, and our environment.

Congress is more than qualified for such a task. It has a long history of addressing threats to privacy exploited by new technologies, such as the Telecommunication Act's restrictions on disclosure of customer proprietary network information and the Right to Financial Privacy Act's constraints on disclosure of consumer bank records.[123]

Congress is better suited for this task than are state or local governments. A more local approach to regulation may allow

120. This is evidenced by customer and community refusal of smart meter devices hindering the progress of the smart grid. *See, e.g.*, Ojai, Cal., Ordinance No. 823, § 1 (May 29, 2012); Naperville Smart Meter Awareness v. City of Naperville, 69 F. Supp. 3d 830, 836 (N.D. Ill. 2014); Nunez, *supra* note 8; Wells, *supra* note 11.

121. *See Naperville*, 69 F. Supp. 3d at 840.

122. *See, e.g.*, American Recovery and Reinvestment Act, Pub. L. No. 111-5, 123 Stat. 115 (2009) (codified as amended in scattered Sections of 6, 19, 26, 42, and 47 U.S.C.).

123. 47 U.S.C. § 222 (2012); 12 U.S.C. §§ 3401–21 (2012).

regulators to tailor privacy controls to the unique energy structures of each state and to work more closely with public utilities, private utilities, and PUCs to find the optimal balance between privacy and smart grid goals. However, as the country moves towards the adoption of a smart grid, our energy system is becoming increasingly national in scope, increasing the need for uniform federal regulation.

By taking the lead on privacy protections for smart meter data, Congress can provide guidance to stakeholders operating in an area of complex and overlapping interests and regulatory authority. Congressional guidance on this issue would enjoy support from both consumers and industry. Utilities will appreciate the federal government stepping in and establishing a uniform standard. Utilities that operate in multiple states, in particular, find adherence to different state regulations onerous.[124] For customers, meanwhile, an uneven patchwork of state and local regulations means that existing privacy protections are largely a matter of geographic happenstance. A uniform federal legislation will maximize the potential of the smart grid by deterring states, like New Hampshire, from free riding by reaping the benefits of other states' investment in the smart technology while their own antiquated infrastructures create an enormous drain on our energy grid.

Further, compared to the federal government, states and PUCs are ill-equipped to regulate these privacy concerns. Because smart meter data are transmitted across state lines, the federal government can regulate them under its Commerce Clause jurisdiction.[125] Meanwhile, state public utility commissions cannot assert legal authority over all potential third-party providers, and state legislatures are unable to effectively protect privacy beyond their borders.

B. Regulating Distribution: Adopting the Colorado Model

It is important for people to understand that smart meters are not, in fact, a plot by the government to spy on us.[126] Smart meters serve an important role in protecting and enhancing our electric grid. In order to address consumer concerns, the Government must heighten privacy controls without sacrificing smart grid potential.

---

124. *See, e.g.*, Mark Seward, *Smart Grid Data—The "Wild West" of Privacy Rights,* SPLUNK BLOGS (May 27, 2011), http://blogs.splunk.com/2011/05/27/smart-grid-data-thewild-west-of-privacy-rights [https://perma.cc/E58X-2H6D].

125. *See, e.g.*, Letter from David K. Owens, Exec. Vice President, Edison Elec. Inst. et al., to the Office of the General Counsel, U.S. Dep't of Energy 10 (July 12, 2010).

126. Nunez, *supra* note 8. Utility workers in Pennsylvania are calling widespread smart meter installation "a plot by Obama to spy on us." *Id.*

This can be accomplished by shifting the conversation from regulation of *installation* to regulation of *distribution*. Law enforcement's access to these data defies customers' reasonable expectations and poses the true threat, which is not the existence and collection of the data themselves. Utility companies have had access to social security numbers, bank account information, and addresses for decades;[127] yet, mandatory access to this highly personal information does not elicit the same kind of panic, because the distribution of this information is highly regulated. Similarly, regulating *access* to smart meter data, rather than focusing on installation, will make the smart meter itself safer without sacrificing smart grid potential.

Generally, energy utilities are required to obtain customer consent before disclosing individual billing information.[128] Smart meter data should be similarly regulated. However, there should be a carve-out for programs necessary to achieve smart grid goals. Further, aggregated data, which pose only a negligible threat to privacy, should be subject to fewer privacy constraints. A successful smart meter data protection regime requires customer consent for the transmission of customer-specific data to third parties, except in those instances where third parties are operating under the supervision of utilities to carry out essential grid operating functions.

Traditionally, personal data are organized into three types: (1) customer-specific data, (2) customer-specific deidentified data, and (3) aggregated data representing community level information.[129] The Colorado PUC calibrates protection measures to the level of risk posed by different types of data in an attempt to maximize the benefits that disclosure of less sensitive data can offer.[130] In doing so, they have created an effective model that should be replicated on a national level.

Customer-specific data generate the greatest privacy concern because they contain personal information that can be traced back to specific individuals and households. They should be afforded the most protection.[131] In Colorado, "a utility is only authorized to use customer data to provide regulated utility service in the ordinary course of

127. *See* Balough, *supra* note 34, at 182.

128. *See id.* at 181–82.

129. *See* Harvey, *supra* note 18, at 2085.

130. *See generally* 4 COLO. CODE REGS. § 723-3 (LexisNexis 2016).

131. This approach has been successfully adopted in Vermont, where eEnergy Vermont requires consent for disclosure of all customer-specific data. *See* INST. FOR ENERGY & THE ENV'T, VT. LAW SCH., CVPS SMARTPOWER: A SMART GRID COLLABORATION IN VERMONT 23 (2012), http://www-assets.vermontlaw.edu/Assets/iee/CVPS-SmartGrid-Report-Final-120215.pdf [https://perma.cc/K26J-6T68].

business."[132] The Colorado PUC defines "the ordinary course of business" as "in furtherance of predefined smart grid goals,"[133] thus ensuring that customer specific data are used exclusively for purposes that align with consumer's reasonable expectations.

Furthermore, in Colorado, a utility may not disclose customer data to any third party, including a government agent, unless the customer first submits a signed "consent to disclose customer data form."[134] Once again, the rule creates a narrow exception for regulators and utility contractors authorizing them to use this data specifically and exclusively in furtherance of predefined smart grid goals.[135] Otherwise, utilities are not allowed to disclose customer data, "except as required by law or to comply with Commission rule."[136] As a result, government officials cannot access consumer data without a warrant, a subpoena, or a court order, further aligning with reasonable expectations of privacy.

As the name suggests, customer-specific deidentified data are customer-specific usage data that have been stripped of all personally identifying information but still indicate single home usage.[137] They should be held to the same standard as consumer-specific data, because they can be manipulated to reidentify individuals and households.[138] It is impossible to tell if data have been sufficiently deidentified because the ability to reidentify data is dependent on the various external databases available to match against smart meter data.[139] Additionally, the technological ability to manipulate data is

---

132. 4 COLO. CODE REGS. § 723-3:3027(a) (LexisNexis 2016).

133. 4 COLO. CODE REGS. § 723-3:3029 (LexisNexis 2016).

134. 4 COLO. CODE REGS. § 723-3:3031 (LexisNexis 2016).

135. 4 COLO. CODE REGS. § 723-3:3029 (LexisNexis 2016). Under California's privacy rules, customer-specific data may also be used without consent only for programs necessary to grid operation that the CPUC, utilities, or third parties under contract with utilities carry out. All other uses require customer consent. *See generally* Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company, Rulemaking 08-12-2009 (Cal. Pub. Util. Comm'n May 6, 2011), http://docs.cpuc.ca.gov/PublishedDocs/PUBLISHED/GRAPHICS/140370.pdf [https://perma.cc/KD8M-FNSF].

136. 4 COLO. CODE REGS. § 723-3:3030(a) (LexisNexis 2016) ("This includes responses to requests of the Commission, warrants, subpoenas, [or] courts orders.").

137. *See* Harvey, *supra* note 18, at 2087.

138. There is a growing consensus that "anonymizing data to sufficiently prevent reidentification of an individual is almost impossible." *See id.* at 2088 (quoting Admin. L. J.'s Ruling Adding Technical Memos to the Record, Rulemaking 08-12-009, at 5 attach. B (Cal. Pub. Util. Comm'n May 13, 2013), http://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M064/K670/64670678.pdf [https://perma.cc/4VBC-KJTT]).

139. *See* Opening Comments of the Electronic Frontier Foundation on Energy Data Center, Rulemaking 08-12-009, at 9 (Cal. Pub. Util. Comm'n Dec. 17, 2012),

constantly changing, creating a genuine concern that data sufficiently deidentified today may be reidentifiable tomorrow.[140] Consequently, Colorado recognizes that deidentified data present the same threat to privacy as customer data and treats them identically.[141]

Aggregated data, on the other hand, are generally considered more secure and, therefore, warrant less protection.[142] Aggregated data are the least invasive because they represent usage at the community, rather than individual, level.[143] As a result, aggregated data should be exempt from consent requirements.[144] In Colorado, utilities can share aggregated data with third parties as long as the "utility takes steps to ensure the report is sufficiently anonymous in its aggregated form so that any individual customer or reasonable approximation thereof cannot be determined from the aggregated amount."[145] To ensure personally identifying data are sufficiently aggregated, Colorado employs a fifteen/fifteen rule. Under this rule, at least fifteen customers must be included in the data, and no single customer can account for more than 15 percent of the group.[146]

The Colorado policy is laudable because it protects tiered reasonable expectations of privacy without sacrificing smart grid potential. With these distribution protections in place, privacy concerns should be mitigated for many customers, resulting in widespread smart meter adoption, ushering our grid into the twenty-first century without sacrificing consumer privacy.

VI. CONCLUSION

Smart meters are integral to the health of the United States' current electric grid and are critical to a reliable, affordable, and efficient energy economy. Effectively implementing smart meters and smart technology will be critical if the United States is to meet the challenges posed by its aging electricity infrastructure. Smart meter technology is creating a new era of consumer behavior geared towards

---

http://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M042/K160/42160299.pdf [https://perma.cc/TT78-PF7C].

140. *See id.* at 34.

141. 4 COLO. CODE REGS. § 723-3:3026(a) (LexisNexis 2016).

142. *See* Harvey, *supra* note 18, at 2089–90.

143. *See id.*

144. For example, the California PUC exempts aggregated data that do not contain personal identifying information; they are specifically exempt from the Commission's Privacy Rules. *See* Audrey Lee et al., Energy Data Center Briefing Paper 1 (2012), http://www.cpuc.ca.gov/NR/rdonlyres/8B005D2C-9698-4F16-BB2B-D07E707DA676/0/EnergyDataCenterFinal.pdf [https://perma.cc/M3Y7-YFTD].

145. *See* 4 COLO. CODE REGS. § 723-3:3032 (LexisNexis 2016).

146. *See id.*

efficiency and conservation. Utilities are increasingly able to offer more affordable, reliable service, and entire new sectors of the economy are emerging as entrepreneurs recognize opportunities in the evolving energy arena. Utilities and regulators are increasingly aware of and able to defend against cyber attacks through situational awareness of the grid. Finally, a broad range of social benefits, environmental and otherwise, will be realized through reduced energy consumption and the introduction of clean energy technologies.

While there are serious potential privacy risks associated with such a transformation, we must not lose sight of the fact that it is smart meter data that pose the threat to privacy, not smart meters themselves. We need to stop trying to limit smart meter installation, and instead limit how we make the data available. We need to make conscious choices about who we want accessing the data and how we want the data to be used. In this way, we can maximize smart grid goals without sacrificing privacy.

Megan McLean[*]

[*] J.D. Candidate, Vanderbilt Law School, 2016; B.A., Environmental Biology, Washington University in St. Louis, 2012. The author would like to thank the editors of the VANDERBILT JOURNAL OF ENTERTAINMENT & TECHNOLOGY LAW for their patience and insightful feedback and her friends and family for their constant support.