Harvard Journal of Law & Technology
Volume 25, Number 1 Fall 2011

PRIVACY AND THE MODERN GRID

*Sonia K. McNeil**

TABLE OF CONTENTS

I. INTRODUCTION

The American electrical grid is in bad shape. Because of chronic underinvestment in research and development,[1] a digital nation now relies on an infrastructure created before the invention of micropro-

* J.D. Candidate 2012, Harvard Law School. Grateful thanks to Judge Alex Kozinski, to Professors Philip Heymann, Charles Nesson, John Palfrey, and Jonathan Zittrain, and to Kevin Bankston, Will Carson, Sachin Desai, Joe Hayes, Meghan Heesch, Bob Herd, Megan Hertzler, David Kessler, Paul Kominers, Abby Lauer, Adam Lewin, Richard and Deborah McNeil, Alan Rozenshtein, Diane Snyder, and Lee Tien. All views and errors are my own.

1. LITOS STRATEGIC COMMC'N, THE SMART GRID: AN INTRODUCTION 6 (2008), http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf [hereinafter THE SMART GRID: AN INTRODUCTION].

cessors[2] that is beginning to show its age. Power quality problems and system disturbances cost the United States nearly $150 billion each year,[3] regional blackouts aggravate and endanger millions of residents,[4] and structural insecurities tempt hackers and terrorists around the globe.[5]

To address these problems, the modern grid is being transformed from an outmoded, centralized network dominated by energy producers to a flexible, decentralized system that is more secure, more reliable, and better able to respond to and interact with consumers.[6] The updated "smart grid" will permit "a two-way flow of electricity and information" in near-real time,[7] creating an adaptive, interactive energy matrix.[8] For consumers, the most visible part of the smart grid will be "smart meters," advanced electrical meters that collect highly granular data on individual electricity consumption[9] and allow users to monitor and remotely control their electrical use[10] in response to fluctuating energy prices.[11] At the level of an individual home, the goal is to use data to encourage consumers to conserve energy by showing them its cost as they use it, rather than days or weeks later in an energy bill.[12] System-wide, this information will be harnessed to

---

2. *Id.* at 7–8.

3. *Id.* at 5; *see also* NAT'L ENERGY TECH. LAB., U.S. DEP'T OF ENERGY, MODERN GRID BENEFITS 4 (2007), http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/Modern%20Grid%20Benefits_Final_v1_0.pdf.

4. In 2008, the Office of Electricity Delivery and Reliability estimated that there had been five "massive blackouts" in the preceding four decades. Three of these blackouts occurred in the nine years leading up to its report. The average outage occurring between 1996 and 2000 affected 409,854 consumers. THE SMART GRID: AN INTRODUCTION, *supra* note 1, at 7.

5. *See* Noah Shachtman, *CIA: Hackers Shook Up Power Grids*, WIRED DANGER ROOM (Jan. 19, 2008, 11:58 AM), http://www.wired.com/dangerroom/2008/01/hackers-take-do.

6. THE SMART GRID: AN INTRODUCTION, *supra* note 1, at 10.

7. *Id.* at 13.

8. For a diagram illustrating one conceptualization of the smart grid, see RICHARD J. CAMPBELL, CONG. RESEARCH SERV., R41886, THE SMART GRID AND CYBERSECURITY — REGULATORY POLICY AND ISSUES 4 (2011).

9. *See How Smart Meters Work*, CENTERPOINT ENERGY, http://www.centerpointenergy.com/services/electricity/business/advancedmetering/howsmartmeterswork (last visited Dec. 21, 2011).

10. *See What is a Home Area Network?*, CENTERPOINT ENERGY, http://www.centerpointenergy.com/services/electricity/business/advancedmetering/faq/#39 (last visited Dec. 21, 2011). Smart meters can communicate with household climate-control systems and smart-meter-compatible appliances through the residence's home area network. *Id.* Whirlpool, one major appliance manufacturer, has stated that it has "committed to make all of its appliances smart grid-compatible by the end of 2015." *What's a Smart Grid? Most Consumers Still Fuzzy on the Concept*, SMARTGRIDNEWS.COM (Mar. 29, 2011), http://www.smartgridnews.com/artman/publish/news/Smart-grid-technology-Most-consumers-still-fuzzy-on-the-concept-3582.html. For an interactive graphic illustrating the operation of a home area network, see *Smart Meter: How a Home Area Network Works*, SAN DIEGO GAS & ELEC., http://rearchive.sdge.com/smartmeter/HANInteractive.shtml (last visited Dec. 21, 2011).

11. SMART ENERGY METERS, http://smartenergymeters.net (last visited Dec. 21, 2011).

12. *See* THE SMART GRID: AN INTRODUCTION, *supra* note 1, at 12. The capacity of individual meter models to show usage in real time varies. In general, however, any delay will

spur economic growth, conserve the environment, increase electrical service reliability, strengthen national security, and develop derivative technologies.[13]

The nationwide deployment of smart meters has begun.[14] This transition, however, brings new threats to privacy. The smart grid's essential innovation is information.[15] From a privacy standpoint, this signature benefit is also the smart grid's Achilles' heel.[16] Because smart meter data is highly granular, it is highly revealing.[17] Data from a smart meter can tell an observer much more about a home than the information from a more traditional meter using older technology.[18]

Fully realizing the benefits of the smart grid, however, requires bringing advanced meters into as many homes and businesses as possible.[19] As a result, it is unlikely that customers will be permitted to opt out of smart meter installation.[20] To date, approximately two mil-

---

be measured in minutes rather than hours or days, as is typically the case with more traditional meters. *See also infra* note 18.

13. *See* NAT'L ENERGY TECH. LAB., U.S. DEP'T OF ENERGY, A VISION FOR THE SMART GRID 5–8 (2009), http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/Whitepaper_The%20Modern%20Grid%20Vision_APPROVED_2009_06_18.pdf; *see also infra* note 30.

14. *See Secretary Chu Announces Two Million Smart Grid Meters Installed Nationwide*, U.S. DEP'T OF ENERGY (Aug. 31, 2010, 12:00 AM), http://energy.gov/articles/secretary-chu-announces-two-million-smart-grid-meters-installed-nationwide.

15. Kevin L. Doran, *Privacy and Smart Grid: When Progress and Privacy Collide*, 41 U. TOL. L. REV. 909, 910 (2010).

16. *Id.*

17. *See infra* Part II.

18. Some electric meters and devices, despite not being "smart," may now collect information more often than once per month, increasing data granularity and potentially triggering privacy concerns. This Note recognizes this complexity but nonetheless treats smart meters as a distinct technological class for two reasons. First, smart meters are uniformly more advanced than traditional meters, and the information that smart meters generate is more refined. Second, smart meters are only one component of the broader transition to the smart grid. This effort, in contrast with past upgrades, is intended to alter permanently the prevailing technological standard for electric meters. The technology's sophistication and its saturation are each relevant to privacy.

19. *See, e.g.*, Letter from David K. Owens, Exec. Vice President, Edison Elec. Inst. et al., to Office of the General Counsel, U.S. Dep't of Energy 15–16 (July 12, 2010) (providing comments in response to the Department of Energy's Request for Information, "Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy") [hereinafter DOE RFI], *available at* http://www.doe.gov/sites/prod/files/gcprod/documents/EdisonElectric_Comments_DataAccess.pdf.

20. *See id.* While a customer could object to smart meter installation, the rules promulgated by state public utility commissions determine whether that objection has legal effect. Utilities may control the type of technology used to deliver or measure service as a matter of their business discretion, and the utility's choice of equipment will be upheld absent a showing of abuse of that discretion. *See* Pub. Serv. Co. v. Pub. Util. Comm'n, 653 P.2d 1117, 1123 (Colo. 1982). Moreover, even if a customer were permitted to opt out of smart meter installation as a legal matter, his or her choice can in practice only be honored so long as their chosen alternative remains both available and technologically compatible with the electric grid, which is itself also in transition. The California Public Utilities Commission appears to be unique in its consideration of a proposal to permit customers to request that the communication functionality of their smart meters be disabled in exchange for an up-

lion smart meters have been installed nationwide.[21] Forty million homes will be equipped with smart meters by 2015.[22] These meters are a rich source of information that is not clearly covered by "existing, sector-specific Federal privacy statutes."[23]

To protect individual privacy and ensure consumer trust during the deployment of smart meter technology, it is vital that an individual's smart meter data be protected from suspicionless access by law enforcement. Despite growing concern about access by law enforcement to other types of sensitive information, however,[24] the prospect of unconstrained law enforcement access to smart meter data has received relatively little attention.[25] This may be because the technology is not well understood.[26] At last count, only four percent of Americans had heard of the smart grid.[27] Nearly half of respondents to another recent survey reported that their community does not understand the technology "at all."[28] Although fully achieving the benefits of the smart grid requires mass deployment of smart meters, the social value that the smart grid creates should not come at the cost of individual privacy.

---

front fee and an additional monthly service charge. *See* Alejandro Lopez de Haro, *PG&E to Now Offer Opt Out Smart Meter Option*, CAPITOLA-SOQUEL PATCH (Aug. 6, 2011), http://capitola.patch.com/articles/pge-to-now-offer-opt-out-smartmeter-option-2.

21. *Secretary Chu Announces Two Million Smart Grid Meters Installed Nationwide*, *supra* note 14.

22. Memorandum from the Vice President to the President, Progress Report: The Transformation to a Clean Energy Economy 5 (Dec. 15, 2009), http://www.whitehouse.gov/administration/vice-president-biden/reports/progress-report-transformation-clean-energy-economy [hereinafter Progress Report].

23. NAT'L SCI. AND TECH. COUNCIL, A POLICY FRAMEWORK FOR THE 21ST CENTURY GRID: ENABLING OUR SECURE ENERGY FUTURE 46 (2011), http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf; *see also* Cheryl Dancey Balough, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161, 176–83 (2011) (discussing the Privacy Act, the Computer Fraud and Abuse Act, Section 5 of the FTC Act, the Wiretap Act, and the Stored Communications Act and concluding that these statutes "do not adequately protect electric consumers").

24. *See* Declan McCullagh, *Geo-privacy bills aim to curb warrantless tracking*, CNET (June 15, 2011, 4:19 PM), http://news.cnet.com/8301-31921_3-20071409-281/geo-privacy-bills-aim-to-curb-warrantless-tracking.

25. The private sector continues to discuss its responsibility to protect privacy, but the dialogue to date has focused primarily on limiting access to and resale of consumer data by other private parties rather than on access by law enforcement. *See, e.g.*, H. Russell Frisby, Jr. & Jonathan P. Trotta, *The Smart Grid: Data Privacy and Security*, 19 COMMLAW CONSPECTUS 297 (2011), http://commlaw.cua.edu/res/docs/05-v19-2-Frisby-Final.pdf (discussing efforts to develop consumer privacy standards for industry and describing the complex environment in which these conversations take place).

26. Andrew Nusca, *Majority of Americans Don't Understand Smart Grid, Study Says*, SMARTPLANET (Mar. 29, 2011, 7:39 AM), http://www.smartplanet.com/blog/smart-takes/majority-of-americans-dont-understand-smart-grid-study-says/15146.

27. Press Release, GE, National Survey: Americans Feel a Smart Grid Will Help Reduce Power Outages, Personal Energy Usage (Mar. 23, 2010), http://www.genewscenter.com/Press-Releases/National-Survey-Americans-Feel-a-Smart-Grid-Will-Help-Reduce-Power-Outages-Personal-Energy-Usage-26c9.aspx.

28. Nusca, *supra* note 26.

This Note discusses two potential sources of privacy protection for an individual's smart meter data: the courts, through the Fourth Amendment, and Congress, through new federal privacy legislation. It proceeds in four parts. Part II introduces the smart grid and smart meter technology, and explains why privacy protections for an individual's smart meter data are critical. Part III discusses the Fourth Amendment and the Fourth Amendment's "third-party doctrine," which generally eliminates constitutional constraints on law enforcement access to information held by third parties. This Part describes the third-party doctrine and explains why it should not be interpreted to remove Fourth Amendment protections for an individual's smart meter data. The Supreme Court, however, has been reluctant to reexamine the third-party doctrine. As a result, Part IV proposes legislative alternatives. This Part identifies and discusses two existing federal legislative frameworks that could be adapted to provide individual privacy protections for smart meter data. Part V concludes.

II. THE SMART GRID AND THE CASE FOR SMART METER DATA PRIVACY

Homes and businesses will spend more than $500 billion annually on electricity by the year 2030.[29] Smart grid technologies have the potential to reduce this bill more than 4%,[30] or approximately $20.4 billion per year,[31] by enabling consumers to educate themselves about their energy use and adjust their consumption to take advantage of fluctuating energy prices. The American Recovery and Reinvestment Act's[32] $4 billion investment in smart grid technology, combined with private capital, is expected to create 104,000 new jobs.[33] Millions of smart meters are already in U.S. homes.[34] Once deployed nationwide,

29. *See Secretary Chu Announces Two Million Smart Grid Meters Installed Nationwide*, *supra* note 14.

30. Power is more expensive at high demand times because it costs more to produce at those times. To minimize energy costs and environmental impact, utilities typically build some power plants that run constantly ("base load plants") and others that operate only during high demand times ("peaking plants"). When consumers and businesses shift their use to lower-demand times of day, energy prices decrease because fewer peaking plants need to be built or operated. Appliance manufacturers will adapt to the smart grid by developing programmable equipment that can be set automatically to perform tasks at low-demand times. *See, e.g.*, Michael Kannellos, *Smart Appliances: What to Expect*, GREENTECH MEDIA (Feb. 5, 2010), http://www.greentechmedia.com/articles/read/smart-appliances-what-to-expect.

31. *Secretary Chu Announces Two Million Smart Grid Meters Installed Nationwide*, *supra* note 14.

32. 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.).

33. *See* Progress Report, *supra* note 22, at 4.

34. *Secretary Chu Announces Two Million Smart Grid Meters Installed Nationwide*, *supra* note 14.

these meters could help consumers to eliminate 442 million metric tons of carbon emissions, equivalent to permanently closing sixty-six coal-fired power plants.[35] The smart grid is expected to make the American power infrastructure not only greener, but also more resilient to power disturbances, natural disasters, and physical attacks.[36] The stakes, in short, are high economically, environmentally, and in terms of national security.

The stakes are also high, however, for individual privacy. The information generated by smart meters creates individual privacy concerns because household energy consumption, particularly when measured in near-real time and traced back to its sources, tells a startling amount about life and behavior within the home.[37] While a more traditional meter records monthly energy consumption as a single lump figure, smart meters may collect 750 to 3,000 distinct and time-stamped data points per month.[38] Some smart meters record energy usage every fifteen minutes, and advanced versions may shrink this window to as few as six seconds or permit measurement in real time.[39]

This information can be analyzed to reveal medical conditions, criminal activity, and other information about life within the home.[40] Individual appliances and other sources of energy use have unique "load signatures," which are the distinct energy consumption patterns

---

35. *DOE Says Smart Grid Can Reduce Emissions by 12 Percent*, SMARTMETERS.COM (Feb. 2, 2010, 2:43 PM), http://www.smartmeters.com/the-news/798-doe-says-smart-grid-can-reduce-emissions-by-12-percent.html.

36. *See Smart Grid*, U.S. DEP'T OF ENERGY, http://energy.gov/oe/technology-development/smart-grid (last visited Dec. 21, 2011); *see also* Boyd Cohen, *If New York City Becomes the "Smartest" City in the World, How Will It Prepare for Future Hurricanes?*, FAST COMPANY CO.EXIST (Sept. 5, 2011), http://www.fastcoexist.com/1678487/if-new-york-city-becomes-the-smartest-city-in-the-world-how-will-it-prepare-for-future-hurri (describing power outages in New York City during Hurricane Irene and noting, "[i]nstead of [preemptively] shutting down city blocks . . . smart grids would allow utilities to isolate at-risk buildings and easily shut down and restart power"). For a discussion of how the smart grid will "self-heal," see NAT'L ENERGY TECH. LAB., U.S. DEP'T OF ENERGY, ANTICIPATES AND RESPONDS TO SYSTEM DISTURBANCES (SELF-HEALS) (2010), http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/09.02.2010_Anticipates%20and%20Responds%20(Self%20Heals).pdf.

37. *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-the-wild-west-of-privacy-rights (citing Megan J. Hertzler, Assistant Gen. Counsel, Xcel Energy, Seminar at Managing SCADA Network Security Risks: Granular Smart Meter data: Energy usage over time from Data Access and Privacy Issues Related to Smart Grid Technologies (May 26, 2011)) (illustrating how power consumption peaks and patterns can be associated with the use of individual appliances).

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

39. Joel M. Margolis, NEUSTAR, *When Smart Grids Grow Smart Enough to Solve Crimes* 4 (2010), http://www.neustar.biz/php/hello_site/pdf/neustar_wp_when_smart_grids_grow_smart_enough_to_solve_crimes.pdf.

40. Lerner & Mulligan, *supra* note 38, ¶ 41.

specific to each source.[41] A refrigerator, for example, draws power in a different way than a television, a respirator, or high-wattage indoor marijuana "grow lights."[42] When aggregated over time, this data can be used to infer the number of people occupying a home, their mundane or illicit habits, and the rhythm of their movements, both in general and on a particular day.[43] Anyone with access to smart meter data can deduce the "avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics of the customer or the customer's household."[44]

As a result, smart meter data can be helpful in criminal investigations.[45] Law enforcement can use this data as either direct or circumstantial evidence of any number of crimes.[46] The information can be used to identify marijuana "grow houses," sweat shops, or brothels, or to detect violations of housing ordinances or zoning regulations.[47] Highly granular energy records are also a rich source of corroborating and potentially incriminating evidence.[48] The data can disclose fraud,[49] substantiate or disprove an alibi,[50] and suggest whether the home's residents conspired to commit a crime.[51] Smart meter data, in sum, enables law enforcement to detect and prosecute more offenses and to do so more efficiently.

Privacy interests, however, do not evaporate when new technologies are introduced, even when those technologies make it easier for law enforcement to perform its protective role.[52] Privacy, the "control over knowledge about oneself,"[53] is a facet of personal liberty,[54] mor-

---

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

42. *See* Seward, *supra* note 37.

43. *See* Gerald Wynn, *Privacy Concerns Challenge Smart Grid Rollout*, REUTERS (June 25, 2010, 7:09 AM), http://www.reuters.com/article/idUSLDE65N2CI20100625.

44. Smart Grid Data Privacy for Electric Utilities, COLO. CODE REGS. § 723-3 (proposed Nov. 3, 2010).

45. The data is also useful in civil disputes and to insurance carriers, marketers, and employers, among others.

46. *See* Margolis, *supra* note 39, at 4–5.

47. Such as, for example, when a business operates industrial machinery on property that is zoned for residential use. *Id*.

48. *Id.*

49. For instance, do you claim reimbursement for a medical device that your electrical consumption data reveals that you are not actually using?

50. For example, does the data associated with your residence show that you really did come home that night? Did you turn on the lights or the television?

51. For example, the data may reveal that a home security system was disarmed at the time of a burglary.

52. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) (wrestling with "what limits there are upon this power of technology to shrink the realm of guaranteed privacy"); Katz v. United States, 389 U.S. 347, 350 n.5 (1967) ("Virtually every governmental action interferes with personal privacy to some degree. The question in each case is whether that interference violates a command of the United States Constitution.").

53. Charles Fried, *Privacy*, 77 YALE L.J. 475, 483 (1968). One scholar has noted, however, that "[t]he number of definitions of privacy is roughly equivalent to the array of scholars

al autonomy,[55] and democracy.[56] It has been called "central to the attainment of individual goals under every theory of the individual that has ever captured man's imagination."[57] Privacy interests in the home have long received "special deference"[58] because of the home's role as a refuge and the center of family life.[59] In the home, "*all* details are intimate details."[60]

Smart meters will physically be part of the home and record life within it with unprecedented specificity. Smart meter data privacy, therefore, is not solely the concern of those who have something to hide.[61] Some form of privacy protection for an individual's data, whether from Congress or from the courts, is vital to ensuring that the threshold of a home is not reduced to "a meaningless symbol"[62] in the process of securing the smart grid's broader social benefits.

Threats to individual privacy posed by evolving forms of technology are often realized belatedly, forcing Congress and the courts to struggle to keep pace. With smart meter data, however, the concerns are already clear.[63] The modern grid will be the result of a concerted and comprehensive technological overhaul, not a haphazard percolation of new products into scattered homes. This revitalization effort is, at bottom, driven by the realization that the grid cannot continue to support the needs of its users in its current state. It is appropriate to approach the question of individual privacy in a smart grid system with similarly proactivity. Timely discussion can help to ensure that

writing about privacy." Carol M. Bast, *What's Bugging You? Inconsistencies and Irrationalities of the Law of Eavesdropping*, 47 DEPAUL L. REV. 837, 881 (1998). For a partial catalog of scholarly conceptualizations and taxonomies of privacy, *see id.* at 883 n. 438.

54. Fried, *supra* note 53, at 483.

55. Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 444 (1980).

56. *See* United States v. White, 401 U.S. 745, 785–86 n.21 (1971) (Harlan, J., dissenting) ("It is obvious that the political system in each society will be a fundamental force in shaping its balance of privacy, since certain patterns of privacy, disclosure, and surveillance are functional necessities for particular kinds of political regime.").

57. Gavison, *supra* note 55, at 445.

58. McDonald v. City of Chicago, 130 S. Ct. 3020, 3105 (2010) (Stevens, J., dissenting) ("This veneration of the domestic harkens back to the common law."). Indeed, one scholar has characterized Fourth Amendment jurisprudence as one of "housing exceptionalism." Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism and the Fourth Amendment*, 95 CORNELL L. REV. 905, 905 (2010).

59. *See id.* ("[O]ur law has long recognized that the home provides a kind of special sanctuary in modern life.") (citing U.S. CONST. amend. III, IV; Lawrence v. Texas, 539 U.S. 558, 562, 567 (2003); Payton v. New York, 445 U.S. 573, 585–90 (1980); Stanley v. Georgia, 394 U.S. 557, 565–68 (1969); Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965)).

60. Kyllo v. United States, 533 U.S. 27, 37 (2001).

61. For a refutation of the argument that privacy is not threatened if the individual has "nothing to hide," see Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 750 (2007). For a defense of "nothing to hide," see Richard J. Posner, THE ECONOMICS OF JUSTICE 271 (1983).

62. *See* Doran, *supra* note 15, at 918.

63. This is demonstrated by the vigorous discussion among industry stakeholders about restrictions on commercial access to and resale of smart meter data. *See* Frisby & Trotta, *supra* note 25, at 320.

the grid's users — who include the residents of nearly every single home in the United States — emerge from this transition with effective privacy safeguards, as well as improved electrical service.

III. SMART METER DATA AND THE FOURTH AMENDMENT

The Fourth Amendment provides one way to balance individual privacy with law enforcement's legitimate need for access to information. The Fourth Amendment sets limits on law enforcement's investigatory powers, including its ability to obtain data.[64] Fourth Amendment protections "hinge on the occurrence of a 'search,' a legal term of art whose history is riddled with complexity."[65] Until *Katz v. United States*,[66] the Supreme Court generally interpreted the Fourth Amendment to be focused on guarding physical places from scrutiny and limiting the search or seizure of tangible objects.[67] Under this prior framework, unless law enforcement trespassed on or appropriated private property, there was no "search," and thus the Fourth Amendment did not apply.[68]

In *Katz*, however, the Court discarded "talismanic" locus-based protections[69] and reframed constitutional privacy protections in terms of reasonable expectations.[70] "The Fourth Amendment," the Court declared, "protects people, not places."[71] After *Katz*, so long as a person exhibits a subjective expectation of privacy in an object, activity, or statement, and that privacy expectation is one that society finds to be objectively reasonable, the Fourth Amendment protects it from warrantless search.[72]

---

64. The Fourth Amendment states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized.

U.S. CONST. amend. IV.

65. Widgren v. Maple Grove Twp., 429 F.3d 575, 578 (6th Cir. 2005).

66. 389 U.S. 347 (1967). In *Katz*, the Court cemented an expansion of Fourth Amendment protections beyond a property-based model that arguably had already begun in Warden, *Maryland Penitentiary v. Hayden*, 387 U.S. 294 (1967), *Berger v. New York*, 388 U.S. 41 (1967), and *Camara v. Municipal Court*, 387 U.S. 523 (1967).

67. *See* Silverman v. United States, 365 U.S. 505, 506–12 (1961).

68. *See* Goldman v. United States, 316 U.S. 129, 131–35 (1942).

69. *Katz*, 389 U.S. at 350–52 ("In the first place the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area.' . . . [What a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

70. *Id.* at 354–56; *see also id*. at 360 (Harlan, J., concurring) (noting that, under the Fourth Amendment, "a person has a constitutionally protected reasonable expectation of privacy").

71. *Id.* at 351.

72. *Id.* at 361 (Harlan, J., concurring).

The Fourth Amendment's third-party doctrine, however, holds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[73] Thus, information shared with third parties is ineligible for Fourth Amendment protections.[74] This means that when law enforcement officials request information from a third party, rather than gathering the data directly, they generally do not need to justify their reasons for searching, seek a court's permission to begin to search, or obey court-imposed restrictions on how long the search can continue or how detailed it may be.[75] Under the third-party doctrine, in the absence of statutory restrictions,[76] the scope of a search is in practice limited only by the discretion of the police[77] and the third party's willingness to cooperate.[78]

This Section begins by introducing the Fourth Amendment. It then describes the third-party doctrine and explains why the Court's interpretation of it has posed, in short, an "enormous problem"[79] for individual privacy. Next, this Section applies the third-party doctrine to an individual's smart meter data. It examines two conceptualizations of the third-party doctrine, drawn from case law and academic scholarship. Finally, this Section explains why the third-party doctrine should not, under either formulation, be interpreted to defeat Fourth Amendment privacy protections for smart meter data.

---

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

74. *See, e.g.*, *Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

75. *See id.* at 358–59.

76. Such as the Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3421 (2006).

77. *Cf. Katz*, 389 U.S. at 358–59 ("[B]ypassing a neutral predetermination of the scope of a search leaves individuals secure from Fourth Amendment violations 'only in the discretion of the police.'" (citation omitted)).

78. For example, Google, one of the few companies to make a practice of disclosing how it responds to law enforcement requests for information, recently reported that it complied with 94% of the requests for user data it received between July 2010 and December 2010. Andy Greenberg, *Google Hands Over User Data for 94% of U.S. Law Enforcement Requests*, FORBES (June 27, 2011, 12:55 PM), http://www.forbes.com/sites/andygreenberg/2011/06/27/google-hands-over-user-data-for-94-of-law-enforcement-requests. At least one utility, Texas's Austin Energy, reportedly "troll[ed] through thousands of records from across Austin" of utility customers' overall electrical consumption at the behest of law enforcement officials seeking to identify "targets" to pursue. Jordan Smith, *APD Pot-Hunters Are Data-Mining at AE*, THE AUSTIN CHRON. (Nov. 16, 2007), http://www.austinchronicle.com/news/2007-11-16/561535. Drawing broad conclusions about the willingness of utilities and other third parties to cooperate with law enforcement is naturally more difficult. *See* U.S. DEP'T OF ENERGY, DATA ACCESS AND PRIVACY ISSUES RELATED TO SMART GRID TECHNOLOGIES 49 (2010), http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf (summarizing public comments on the question of when and how authorized government agents should gain access to energy consumption data).

79. Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 356 (2008).

A. The Fourth Amendment and Advanced Surveillance Technologies

Like technology itself, Fourth Amendment jurisprudence has evolved in fits and starts.[80] In the forty-odd years since *Katz* was decided, courts have continued to wrestle with the proper way to balance privacy concerns with legitimate law enforcement uses of technology-assisted surveillance.[81] Even as technology has evolved, however, the "reasonable expectation of privacy" has remained "remarkably opaque."[82] The Court uses multiple tests to determine whether an expectation of privacy is "reasonable," and it tends to apply its mélange inconsistently.[83]

Nonetheless, amid this confusion, the home has remained "the realm of guaranteed privacy."[84] Intrusions into the home are "the chief evil against which the wording of the Fourth Amendment is directed."[85] Although the Court has so far permitted relatively unfettered surveillance of a person's movements in public,[86] it has generally required probable cause and a warrant in order to enter a home.[87]

In *Kyllo v. United States*, for example, an agent from the Department of the Interior viewed Danny Kyllo's Oregon residence using a thermal imaging device.[88] The images revealed interior temperatures

---

80. *Compare Katz*, 389 U.S. at 353 (finding warrantless wiretapping of telephone conversations to be a search within the meaning of the Fourth Amendment), *with* Olmstead v. United States, 277 U.S. 438, 464 (1928) ("The Amendment itself shows that the search is to be of material things. . . . The amendment does not forbid [wire tapping]. . . . The evidence was secured by the use of the sense of hearing and that only.").

81. For example, compare *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *cert. granted sub. nom. United States v. Jones*, 131 S. Ct. 3064 (2011) (finding surveillance of a subject's movements, including on public roads, via GPS tracking conducted over twenty-eight days to be a search), with *United States v. Cuevas-Perez*, 640 F.3d 272 (7th Cir. 2011) (finding surveillance of a subject's movements via GPS tracking conducted over sixty hours not to be a search), *United States v. Marquez*, 605 F.3d 604, 609 (8th Cir. 2010) (noting in dicta, "[a] person traveling via automobile on public streets has no reasonable expectation of privacy in his movements from one locale to another."), and *United States v. Pineda-Moreno*, 591 F.3d 1212, 1213 (9th Cir. 2010) (finding surveillance conducted with "various types of mobile tracking devices" over a four-month period not to be a search).

82. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 505 (2007) ("Among scholars, this state of affairs is widely considered an embarrassment. The Court's handiwork has been condemned as 'distressingly unmanageable,' 'unstable,' and 'a series of inconsistent and bizarre results that [the Court] has left entirely undefended.'" (footnotes omitted)).

83. *See generally id.*

84. Kyllo v. United States, 533 U.S. 27, 34 (2001).

85. Payton v. New York, 445 U.S. 573, 585 (1980) (quoting United States v. U.S. Dist. Court, 407 U.S. 297, 313 (1972)).

86. *See* United States v. Knotts, 460 U.S. 276, 281 (1983). *But see Maynard*, 615 F.3d at 563–64. Even surveillance in public places, however, is not completely unconstrained. The Fourth Amendment also obligates the courts "to guard against police conduct which is overbearing or harassing." Terry v. Ohio, 392 U.S. 1, 15 (1968).

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

88. *Id.* at 29.

consistent with the presence of halide lights, often used to grow marijuana.[89] Agent Elliott ultimately proved to be correct both about the lights and the drugs, but the Court found the imaging to be an impermissible warrantless search.[90] To the Court, pointing the thermal imager at Kyllo's house was, for Fourth Amendment purposes, equivaequivalent to entering it.[91] The notion that the thermal imager did not reveal information about the home's interior was, the Court observed, "simply inaccurate."[92]

As the discussion above illustrates, smart meter data reveals far more about the interior of a home and the lives of its residents than the grainy images produced by the device used in *Kyllo*. But, importantly, *Kyllo* considered incriminating information that the government had gathered itself.[93] If law enforcement were able to collect smart meter data directly, it would arguably be a "search" within the meaning of the Fourth Amendment.[94]

Direct law enforcement access to smart meter data, however, is not known presently to be possible.[95] Because of concerns about grid security,[96] it may never be advisable.[97] As a result, investigators will

89. *Id.*

90. *Id.* at 34–35.

91. *Id.* at 34. "[O]btaining 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 — at least where (as here) the technology in question is not in general public use." *Id.* (internal citation and quotations omitted).

92. *Id.* at 35 n.2.

93. *Kyllo*, 533 U.S. at 29–30.

94. *Id.* at 34–35. The Supreme Court of Canada recently considered whether surveillance of a suspect's aggregate energy consumption infringed his right "to be secure against unreasonable search" under Section 8 of the Canadian Charter of Rights and Freedoms. Regina v. Gomboc, [2010] S.C.C. 55, ¶ 74 (Can.). Finding that "[t]he evidence available on the record offers no foundation for concluding that the information disclosed by [the device] yielded any useful information at all about household activities of an intimate or private nature," the Court upheld the defendant's conviction for growing marijuana. *Id* ¶ 16. Notably, however the Court reserved consideration of smart meter data. *Id.* ¶ 40.

95. If advances in surveillance capabilities make this technological assumption untrue, however, the analysis would shift to focus exclusively on the Fourth Amendment rather than on the third-party doctrine.

96. Siobhan Gorman, *Electricity Grid in U.S. Penetrated By Spies*, WALL ST. J., Apr. 8, 2009, at A1, *available at* http://online.wsj.com/article/SB123914805204099085.html (describing a 2009 incident in which "cyberspies . . . penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system").

97. Past efforts by law enforcement to gain access to other vital networks have been met with concern. *See, e.g.*, Charlie Savage, *Wider Web Wiretap Law Is Sought*, N.Y. TIMES, Nov. 17, 2010, at B5 (describing concerns that a proposal to facilitate law enforcement access to information about Internet users would inhibit innovation and be harnessed by repressive regimes to identify political dissidents); *Hearing Before the Subcomm. on Telecomm., Trade, and Consumer Prot. of the H. Comm. on Commerce on the Wireless Privacy Enhancement Act of 1999 and the Wireless Communications and Public. Safety Enhancement Act of 1999*, 106th Cong. (1999) (statement of James X. Dempsey, Senior Staff Counsel, Ctr. for Democracy and Tech.) ("[T]he same backdoors that give law enforcement access create new vulnerabilities for hackers to exploit.").

be forced to turn to utilities and other third parties to retrieve an individual's smart meter data.[98] When law enforcement collects information about an individual from a third party, the Fourth Amendment's third-party doctrine applies.[99]

B. The Fourth Amendment's Third-Party Doctrine

The third-party doctrine states that a person cannot legitimately expect information that is shared with a third party to remain private from law enforcement.[100] Many have argued, sometimes vociferously, that the doctrine should be abandoned or overruled.[101] It is a doctrine that scholars "love to hate,"[102] excoriated[103] as an outmoded relic of a social and technological era[104] that is now long past. Although some lower courts have found Fourth Amendment protections for data held by third parties,[105] these decisions still generally must distinguish the third-party doctrine's seminal cases,[106] which have not yet been overruled.[107] The discussion that follows, therefore, takes the third-party doctrine as given and makes the case for Fourth Amendment protections for an individual's smart meter data notwithstanding its shadow.

To begin, this Section outlines the history of the third-party doctrine, which has fit uncomfortably within Fourth Amendment juris-

---

98. One scholar has dubbed this practice "transaction surveillance." Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139 (2005).

99. *See, e.g.*, United States v. White, 410 U.S. 745, 752 (1971).

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

101. *See, e.g.*, Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 39–40 (2011) (celebrating that the third-party doctrine "has at least taken ill, and it can be hoped it is an illness from which it will never recover"). *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 561 (2009) (arguing that the third-party doctrine serves "critical functions").

102. Kerr, *supra* note 101, at 563.

103. *See, e.g.*, 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(c), at 747 (4th ed. 2004) ("The result reached in [*United States v.*] *Miller* is dead wrong, and the Court's woefully inadequate reasoning does great violence to the theory of Fourth Amendment protection which the Court had developed in *Katz*." (footnote omitted)).

104. *See* Henderson, *supra* note 101, at 45 ("[I]t is in fact technology and associated changes in social norms that have *caused* far more information to reside with third persons than has ever been the case.").

105. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP" and that "to the extent that the [Stored Communications Act ("SCA")] purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional" (internal quotations and citations omitted)).

106. *Id.* (distinguishing United States v. Miller, 425 U.S. 435 (1976)).

107. Some of these cases, however, have provoked a response from Congress. The Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3421 (2006), is one example. This statute was designed to limit the holding in *Miller*. FED. RESERVE BD., CONSUMER COMPLIANCE HANDBOOK: RIGHT TO FINANCIAL PRIVACY ACT 1 (2006), *available at* http://www.federalreserve.gov/boarddocs/supmanual/cch/priv.pdf.

prudence since its inception. Next, it discusses two conceptualizations of the third-party doctrine: first, as a doctrine of reasonableness and second, as a doctrine of consent. This Section concludes that under either formulation, courts should not interpret the third-party doctrine to defeat Fourth Amendment protections for an individual's smart meter data.

1. The Evolution of the Third-Party Doctrine: From Secret Agents to Stored Records

Law enforcement has long used informants and undercover agents, one type of third party, to gather evidence.[108] The earliest Supreme Court challenge to the practice on Fourth Amendment grounds was *On Lee v. United States*.[109] *On Lee* was the first in the line of so-called "secret agent cases,"[110] which together established that law enforcement did not violate the Fourth Amendment by using third parties to obtain information without first seeking a warrant.[111] "[A] wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it," the Court announced, receives no protection under the Fourth Amendment.[112]

The "misplaced belief" rationale of the secret agent cases was subsequently extended to business records.[113] Citing the secret agent cases, the Court in *United States v. Miller*[114] refused to suppress bank records, obtained with a defective subpoena, which corroborated the defendant's intent to defraud the government of the tax owed on his illegal moonshine operation.[115] In "revealing his affairs" to the bank, the Court held, the defendant had assumed the risk that his infor-

108. *See, e.g.*, Sorrells v. United States, 287 U.S. 435 (1932); Gouled v. United States, 255 U.S. 298 (1921). The discussion tracing the history of the third-party doctrine owes much to Kerr, *supra* note 101.

109. 343 U.S. 747 (1952).

110. Kerr, *supra* note 101, at 567.

111. *See* Hoffa v. United States, 385 U.S. 293 (1966); Lewis v. United States, 385 U.S. 206 (1966); Lopez v. United States, 373 U.S. 427 (1963).

112. *Hoffa*, 385 U.S. at 302. The Court stated in *Hoffa* that "[t]he risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society." *Id.* at 303.

113. United States v. White, 401 U.S. 745 (1971). *White* was the first case about third parties decided after *Katz*. Seeing "no indication" in *Katz* that the Court meant to reject *On Lee* or *Hoffa*, the Court applied the "reasonable expectations" rationale of *Katz* and found that "[i]f the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations which are later offered into evidence to prove the State's case." *Id.* at 752. Justice Douglas dissented, writing, "What the ancients knew as 'eavesdropping,' we now call 'electronic surveillance'; but to equate the two is to treat man's first gunpowder on the same level as the nuclear bomb. Electronic surveillance is the greatest leveler of human privacy ever known." *Id.* at 750 (Douglas, J., dissenting).

114. 425 U.S. 435 (1976).

115. *Id.* at 436.

mation would be shared with law enforcement.[116] Phrased in the language of *Katz*, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[117]

2. The Third-Party Doctrine as a Doctrine of Reasonableness

The third-party doctrine, understood as a doctrine of reasonableness, applies the two-part inquiry of *Katz* to decide whether data shared with a third party receives Fourth Amendment protections.[118] In order to determine whether the government's conduct violated a reasonable expectation of privacy and was therefore a "search," the court asks two questions. First, did the individual actually exhibit an expectation of privacy?[119] If so, is that subjective expectation of privacy one which society recognizes as reasonable?[120] Under the third-party doctrine, the Court's answer to the second question has been, almost uniformly, "no."[121]

This binary conception of privacy[122] as "a discrete commodity, possessed absolutely or not at all"[123] has been criticized as unrealistic,[124] undemocratic,[125] and strange.[126] Privacy need not be considered in absolute terms, however. If reasonableness is the "touchstone" of the Fourth Amendment,[127] assessing society's actual attitudes toward the reasonableness of an individual's expectations when disclosing information to a third party seems both wholly appropriate and, as an empirical matter, entirely possible. In its surveillance cases, the Court has repeatedly cautioned, "Fourth Amendment cases must be decided on the facts of each case, not by extravagant generalizations."[128] Though the courts must generalize under the rubric of *Katz*, there is

116. *Id.* at 443.

117. Smith v. Maryland, 442 U.S. 735, 744 (1979) (citing *Miller*, 425 U.S. at 444).

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

119. *Id.* at 361 (Harlan, J., concurring).

120. *Id.*

121. *Smith*, 442 U.S. at 743–44.

122. Doran, *supra* note 15, at 918.

123. *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

124. Richard A. Posner, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 140 (2006) ("Informational privacy does not mean refusing to share information with everyone.").

125. *Cf.* United States v. White, 401 U.S. 745, 785 (1971) (Harlan, J., dissenting) (criticizing the assumption that "uncontrolled consensual surveillance in an electronic age is a tolerable technique of law enforcement, given the goals of our political system.").

126. LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW § 15-16, at 1391 (2d ed. 1988) ("A majority of the Justices apparently confuse privacy with secrecy; yet even their notion of secrecy is a strange one, for a secret remains a secret even when shared with those whom one selects for one's confidences.").

127. *See* Samson v. California, 547 U.S. 843, 855 n.4 (2006).

128. Dow Chem. Co. v. United States, 476 U.S. 227, 239 n.5 (1986).

no requirement that "reasonableness" and "legitimacy" be divorced from reality.[129]

For example, to determine whether an individual has been "seized" within the meaning of the Fourth Amendment, the Court considers whether, under the circumstances, a reasonable person would feel "free to leave."[130] A recent study responded to Justice Breyer's lament that without empirical evidence, he was left to extrapolate reasonableness under the seizure standard from "just one person's instinct."[131] The results of the study raised "troubling questions about the way the Court has protected the rights guaranteed by the Fourth Amendment" as to freedom from unreasonable seizures.[132] If the Court refers to studies like this one in the future, as other courts have done in the past,[133] the Court could inform its application of the reasonableness standard and reach a result that accounted for, or at least acknowledged, actual social consensus.

This approach would not be novel. Courts have considered public opinion[134] or turned to statistics[135] in contexts beyond the Fourth Amendment, both to ground the rationale of holdings[136] and to better understand their practical effects.[137] Survey evidence about individual

---

129. *Cf.* Smith v. Maryland, 442 U.S. 735, 750 (Marshall, J., dissenting) (arguing, "[s]ince it is the task of the law to form and project, as well as mirror and reflect, we should not . . . merely recite . . . risks without examining the desirability of saddling them upon society" (alterations in original) (quoting *White*, 401 U.S. at 786 (Harlan, J., dissenting))); Janice Nadler, *No Need to Shout: Bus Sweeps and the Psychology of Coercion*, 2002 SUP. CT. REV. 153, 156 ("[T]he Court's Fourth Amendment consent jurisprudence is either based on serious errors about human behavior and judgment, or else has devolved into a fiction of the crudest sort . . . .").

130. United States v. Medenhall, 446 U.S. 544 (1980).

131. David K. Kessler, *Free to Leave? An Empirical Look at the Fourth Amendment's Seizure Standard*, 99 J. CRIM. L. & CRIMINOLOGY 51, 51 (2009).

132. *Id.* at 54.

133. *See* United States v. Maynard, 615 F.3d 544, 552 (D.C. Cir. 2010); State v. Harrington, 222 P.3d 92, 96 n.4 (Wash. 2009).

134. For example, courts regularly refer to surveys to assess whether there has been consumer confusion, which is relevant to issues ranging from the First Amendment and commercial speech to trademark infringement. *See, e.g.*, Mattel, Inc. v. Azrak-Hamway Int'l, Inc., 724 F.2d 357, 361 (2d Cir. 1983) ("[A] usual way to demonstrate either consumer confusion or secondary meaning . . . is for the proponent to undertake some form of survey of consumer attitudes under actual market conditions.").

135. *See, e.g.*, Padilla v. Kentucky, 130 S. Ct. 1473, 1485 (2010) ("[P]ractice has shown that pleas are less frequently the subject of collateral challenges than convictions obtained after a trial. Pleas account for nearly 95% of all criminal convictions. But they account for only approximately 30% of the habeas petitions filed.").

136. For example, the court in Graham v. Florida, 130 S. Ct. 2011 (2010), held:

The available data, nonetheless, are sufficient to demonstrate how rarely these sentences are imposed . . . . [T]he comparison suggests that in proportion to the opportunities for its imposition, life without parole sentences for juveniles convicted of nonhomicide crimes is as rare as other sentencing practices found to be cruel and unusual.

Id. at 2024–25.

137. *See, e.g.*, Melendez-Diaz v. Massachusetts, 129 S. Ct. 2527, 2537 (2009) ("One study of cases in which exonerating evidence resulted in the overturning of criminal convic-

privacy expectations in electrical consumption information is available.[138] One such study asked participants to rank the "relative intrusiveness" of twenty-five types of law enforcement investigation on a scale of one to one hundred.[139] Participants gave the data generated by traditional meters[140] an average intrusiveness rating of 57.5, reporting that access by law enforcement to electricity records would feel more intrusive than access to criminal, traffic, or real estate records,[141] but less intrusive than access to credit card records.[142] Consumers can be expected to feel that smart meter data, which reveals far more about the home than traditional meter data,[143] is even more sensitive. Indeed, seventy-nine percent of respondents to one industry survey stated that they believe "only customers and utilities should have access to smart meter information."[144]

In sum, the Court's interpretation of the third-party doctrine has fallen out of step with the "reasonable expectations" of the people whom the Fourth Amendment protects. Empirical evidence offers one way to resolve the dissonance between the Court's opinion and public opinion.[145] With smart meter data, the consensus seems clear. The third-party doctrine, understood as a doctrine of reasonableness, should not be interpreted to strip an individual of Fourth Amendment protections for his or her smart meter data.

---

tions concluded that invalid forensic testimony contributed to the convictions in 60% of the cases.").

138. *See, e.g.*, Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 336 (2008) ("These empirical observations [in the author's survey] suggest that . . . . the important variable appears to be the nature of the [personal] record, not who or what institution possesses it.").

139. *Id.* at 333. Notably, participants in the study ranked many types of requests for records as more highly intrusive than patdowns, which require reasonable suspicion, or car searches, which require probable cause. *Id.* at 335.

140. Slobogin's survey did not specify whether "electricity records" were records that included smart meter data or more traditional meter data. It is almost certain, however, that the responses he collected contemplated traditional meter data. Slobogin administered the survey to a Gainesville, Florida jury pool some time before 2008. *Id.* As of Nov. 15, 2010, smart meters had not been installed in Gainesville. Steve Stewart, *Tallahassee Leads in Smart Meter Spending*, TALLAHASSEE REP. (Nov. 15, 2010), http://tallahasseereports.com/2010/11/15/tallahassee-leads-in-smart-meter-spending.

141. These records received mean intrusiveness ratings of 36.2 and 45.5, respectively. Slobogin, *supra* note 138, at 335.

142. Credit card records received a mean intrusiveness rating of 75.3. *Id.*

143. *See* text accompanying notes 37–39.

144. DOE RFI, *supra* note 19, at 9. EEI's survey methodology is not discussed in its comments, making it unclear whether law enforcement access to smart meter information was explicitly raised. *Id.* Even so, the results are suggestive.

145. *See* Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727, 732 (1993) ("[I]f one takes the Justices at their word, a sense of how (innocent) U.S. citizens gauge the impact of police investigative techniques on their privacy and autonomy is highly relevant to current Fourth Amendment jurisprudence.").

3. The Third-Party Doctrine as a Doctrine of Consent

Understood as a doctrine of reasonableness, as discussed above, the third-party doctrine answers "no" to the question, "Can a person who shares information with a third party reasonably expect that it will remain private?"[146] Framed as a doctrine of consent, the question is instead, "When does a person's choice to disclose information to a third party constitute consent to a search by law enforcement?"[147] The distinction is not merely semantic. While a search conducted with consent may still violate an expectation of privacy, when permission is given the violation is considered to be constitutionally reasonable.[148] By one estimate, "[o]ver 90% of warrantless police searches are accomplished" via consent.[149]

Even when a person allows a third party access to information, however, it does not necessarily mean that either the individual or the third party has consented to access by the government.[150] Understood as a doctrine of consent, 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. With smart meter data, both assumptions fail.

A. The Choice to Disclose

We are profligate sharers of data.[151] For some categories of information, sharing is clearly a deliberate choice.[152] For smart meter data, however, the "choice" is harder to find. As one scholar has put it, "[l]iving without basic utility services such as electricity or water, and keeping one's savings in a shoebox rather than a bank" may be "certainly within the realm of the possible," but it is "not within the

146. Kerr, *supra* note 101, at 563.

147. *Id.* at 588.

148. Georgia v. Randolph, 547 U.S. 103, 109 (2006); *see also* Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) ("[O]ne of the specifically established exceptions to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent.").

149. Ric Simmons, *Not "Voluntary" but Still Reasonable: A New Paradigm for Understanding the Consent Searches Doctrine*, 80 IND. L.J. 773, 773 (2005). Simmons notes that "[s]ome estimates are even higher." *Id.* at 773 n.1.

150. *But see* Kerr, *supra* note 101, at 590 ("This is a fair point. . . . [but] it is also a narrow one.").

151. Alex Kozinski & Stephanie Grace, *Remember what the Fourth Amendment protects? No? Just as well.*, AXIS OF LOGIC (June 22, 2011), http://axisoflogic.com/artman/publish/Article_63269.shtml.

152. *Id.* ("It started with the supermarket loyalty programs. They seemed innocuous enough — you just scribble down your name, number and address in exchange for a plastic card and a discount on Oreos.").

realm of the normal."[153] In states with extreme temperatures, living without basic utility services may actually be impossible at times. For this reason, statutes known as "cold weather rules" limit a utility's ability to cut off service during some months, even to a non-paying customer.[154]

Although customers can delay paying their bills in these months, however, they cannot avoid having those bills calculated using information from their electrical meters. Customers cannot bypass electrical meters without risking severe injury, property damage, or death,[155] not to mention criminal penalties.[156] 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.[157]

B. The Limits of Consent

Defenders of the third-party doctrine contend that even if a person gives information to a company without anticipating or intending that it be shared with law enforcement, this "should be irrelevant to whether the consent is valid."[158] This argument still requires, of course, the predicate of having voluntarily shared the information in the first place. Even consent, though, is not unlimited in the law. To take one example, consider the doctrine of unconscionability. It responds to abuses in the contracting process, including "unreasonably or unexpectedly harsh"[159] terms that "seek to negate the reasonable expectations of the nondrafting party."[160] Substantive unconscionability may alone be enough to prompt a court to refuse to enforce a contract.[161]

Initial public reaction to a draft smart meter data sharing consent form proposed by the Colorado Public Utilities Commission offers a glimpse of electric customers' contractual expectations.[162] The form, which must be notarized if submitted on paper rather than electroni-

153. Doran, *supra* note 15, at 919.

154. *See, e.g.*, MINN. STAT. § 216B.097(1) (2010).

155. *See, e.g.*, *Energy Theft & Meter Tampering*, GREENVILLE UTIL., http://www.guc.com/residential/aboutmeters.aspx#energytheft (last visited Dec. 21, 2011) ("Even if the danger does not occur at the time of the theft, the meter is often left in an unsafe condition that is potentially dangerous to others").

156. *See, e.g.*, MINN. STAT. § 609.52 (2010) (defining and providing penalties for theft, including for the theft of electricity).

157. This is particularly true for vulnerable populations dependent on electric service, such as the very young, the very old, the infirm, or their caregivers.

158. *See, e.g.*, Kerr, *supra* note 101, at 588.

159. 8 RICHARD A. LORD, WILLISTON ON CONTRACTS § 18:10 (4th ed. 2011).

160. *Id.*

161. U.C.C. § 2-302(1) (2003).

162. *Energy Lawyer Asks: Can a Data-Use Consent Form Be Too Clear?*, SMART GRID TODAY (May 18, 2011), http://www.smartgridtoday.com/public/2956print.cfm.

cally, allows consumers to authorize smart meter data sharing between their utility and other commercial third parties.[163] It reads, in part, "I understand such data may reveal information about the way I use energy at my premises. Such data can be used to gain personal information, such as what appliances I use and when I use them, as well as when I am at home and when I am away."[164] Some fear that the form "is so effective at disclosing the risk of data sharing that it will likely scare consumers out of sharing any data at all."[165]

This account is anecdotal, but the underlying point remains. Smart meter data is sensitive. While individual attitudes vary, on the whole, Americans tend to be more mistrustful of government access to their information than of access by third parties in the private sector.[166] If fully informed customers would not consent to have their data shared even with other commercial third parties, their "reasonable expectations"[167] are likely to be that the data is kept absolutely private by the utility. The third-party doctrine, therefore, even if understood as a doctrine of consent, should not defeat privacy protections for an individual's smart meter data.

IV. THE CASE FOR SMART METER DATA PRIVACY LEGISLATION

As demonstrated above, the third-party doctrine should not be interpreted to eliminate Fourth Amendment protections for an individual's smart meter data. The third-party doctrine has so far resisted most salvos against it, however.[168] Even if the Supreme Court eventually holds that law enforcement must obtain a warrant in order to access an individual's smart meter data, lack of clear guidance in the interim may prompt fearful utility customers to balk at smart meter installation, delaying or derailing the smart grid. Legislation, therefore, may be the best way both to protect privacy now and to encourage future

---

163. *Id.*

164. *Id.*

165. *Id.* This quote alludes to the interaction between data privacy and competition law. *See generally* Pamela Jones Harbour & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 76 ANTITRUST L.J. 769, 797 (2010).

166. This is particularly true when we are compared to our European counterparts:

> America, in this as in so many things, is much more oriented toward values of liberty, and especially liberty against the state. . . . The prime danger, from the American point of view, is that "the sanctity of [our] home[s]," in the words of a leading nineteenth-century Supreme Court opinion on privacy, will be breached by government actors.

James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161–62 (2004).

167. "Reasonable expectations" here means expectations in the contractual sense, rather than as this phrase is used in Fourth Amendment jurisprudence.

168. *See supra* Part III.B.

courts to join in the effort.[169] After all, the Fourth Amendment is not "the only game in town."[170]

A. The Case for Leadership by Congress

Congress has the ability to categorize some types of information about an individual as private and to regulate law enforcement access to that data, as past legislation shows.[171] It has also played a longstanding role in addressing threats to privacy arising from gaps in laws that are exposed by new technologies, such as through the Telecommunications Act's restrictions on disclosure of customer proprietary network information[172] and the Right to Financial Privacy Act's constraints on disclosure of consumer bank records.[173] Smart meter data will be transmitted across state lines, presenting "a unique set of jurisdictional and practical issues well suited for Federal guidance."[174] In providing this guidance, Congress would enjoy support from both consumers and industry. Utilities are expected to "welcome the federal government stepping in and passing a single privacy standard for this kind of data."[175] Particularly for utilities that operate in multiple states, "adhering to all the state regulations with their nuanced differences" will be onerous.[176] For consumers, meanwhile, an uneven patchwork of state and local regulations means that privacy protections will be largely a matter of geographic happenstance.[177]

Congress both has the authority to regulate this data and is the appropriate body to do so.[178] The federal government is heavily invested in the smart grid,[179] and the health and security of the electrical

169. The existence or absence of legislation offering guidance on privacy can shape judicial thinking on the objective reasonableness of privacy expectations. *See, e.g.*, Payton v. New York, 445 U.S. 573, 598–600 (1980); United States v. Watson, 423 U.S. 411, 421–22 (1976).

170. Kerr, *supra* note 101, at 590 (noting that critics of the Court's Fourth Amendment jurisprudence "suffer from constitutional myopia").

171. *See, e.g.*, Pub. L. No. 104-104, 110 Stat. 56 (1996).

172. 47 U.S.C. § 222 (2006).

173. 12 U.S.C. §§ 3401–3421 (2006).

174. DOE RFI, *supra* note 19, at 10.

175. Seward, *supra* note 37.

176. *Id.* Insofar as this onus translates into costs, utility customers will share the burden, since utility operating expenses are a factor in the calculation of utility rates.

177. *Compare* Smart Grid Data Privacy for Electric Utilities, COLO. CODE REGS. § 723-3 (proposed Nov. 3, 2010) (permitting access by law enforcement on request and without any requirement of preexisting suspicion), *with* Washington Public Records Act, WASH. REV. CODE § 42.56.335 (2010) (prohibiting access unless the agency states in writing that it suspects a crime has been committed and that it has a reasonable belief that the customer records will help to determine if that suspicion is accurate).

178. Moreover, "error costs of legislation may be lower than those of constitutional decision making." Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 595 (2011).

179. *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.).

system directly impacts national security.[180] The deployment of smart meters will also create competing priorities among agencies. If, for example, law enforcement agencies push for unfettered access to smart meter data and discourage consumer adoption of this technology, the goals of the Department of Energy and others will be impaired. State public utilities commissions, meanwhile, cannot assert legal authority over all potential third-party service providers, and state legislatures will be unable to protect privacy effectively beyond their borders. By taking the lead on privacy protections for smart meter data, at least in terms of defining boundaries to access by law enforcement, Congress can provide guidance to stakeholders operating in an area of complex and overlapping interests and regulatory authority.[181]

B. Two Proposals for Legislative Action

Congress has more than once reacted to the Supreme Court's decisions by passing laws that, while falling short of statutorily mandating full Fourth Amendment safeguards, do provide some privacy protections for an individual's sensitive data.[182] Recently, Congress has shown signs of an appetite for even stronger, prospective privacy measures for some types of information.[183] Legislation limiting government access to an individual's smart meter data could take a variety of forms. This Part sketches two possible models and highlights drafting challenges associated with each. The first model bars most law enforcement attempts to access information about an individual that is held by a third party without some form of legal process, albeit less than would be necessary to satisfy the Fourth Amendment. The second model, in contrast, precludes law enforcement access without probable cause and a warrant.

These proposals illustrate the range of safeguards that could preserve individual privacy while remaining flexible enough to accommodate technological change over time. Both proposals grant privacy protections to the individual utility customer in the form of restrictions on access to the individual's data. Defining restraints on access based on the type of data that is generated by the meter and stored by the utility, rather than by the type of meter that is installed,

---

180. *See* Margolis, *supra* note 39, at 5.

181. Congress could either fill in the details itself through legislation or direct an agency to promulgate regulations that obey prescribed parameters. *See, e.g.*, The Secure and Fortify Electronic Data Act of 2011, H.R. 2577, 111th Cong. (2011).

182. FED. RESERVE BD., CONSUMER COMPLIANCE HANDBOOK: RIGHT TO FINANCIAL PRIVACY ACT 1 (2006), *available at* http://www.federalreserve.gov/boarddocs/supmanual/cch/priv.pdf.

183. *See, e.g.*, Geolocational Privacy and Surveillance Act of 2011, S. 1212, 112th Cong. (2011).

allows these proposals to remain effective as technology evolves. Critically, however, their efficacy in translating privacy protections from a legal prescription to a practical reality depends on the basic assumption that smart meter data can be made secure enough to prevent access that circumvents legally mandated processes. While the discussion of the proposals outlined in this Subpart focuses on privacy, not security, the two issues are inextricably linked. Either proposal can easily be defeated if the information that the law seeks to protect is left vulnerable.[184]

1. Proposal One: Require Notice and Provide Standing

The first proposed model for smart meter data privacy legislation is based on the Right to Financial Privacy Act of 1978.[185] The Right to Financial Privacy Act provides a useful framework because it is designed to address individual privacy interests in sensitive information that is stored by third parties. Moreover, the majority of its substantive provisions may easily be modified to suit smart meter data. The Act provides that "no Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution"[186] unless certain conditions are met. These conditions are informed customer consent, an administrative subpoena, a judicial subpoena, a search warrant, or a formal written request, all of which are subject to additional prescriptions.[187] Importantly, the Act also contains "customer challenge provisions,"[188] which give the customer standing to file a motion to quash a subpoena or to prevent the financial institution from fulfilling a formal written request for the information.[189]

The most difficult part of adapting this model to protect an individual's smart meter data, rather than his or her financial records, will be defining the legislation's scope. Much of the debate about drafting likely will center on the definition of the term that replaces "financial institution."[190] The companies and industry groups who identify themselves as stakeholders in consumer data privacy span a broad spec-

184. To illustrate, consider Austin Energy's alleged collaboration with the Austin Police Department. *See* Smith, *supra* note 78. An investigation of the utility's activities revealed evidence that the police had been given their own password to access Austin Energy's customer database. *Id.* Even on less egregious facts, however, effective cybersecurity means effective human security. For more on the smart grid and cybersecurity generally, see CAMPBELL, *supra* note 8.

185. 12 U.S.C. §§ 3401–3421 (2006).

186. *Id.* § 3402.

187. *Id*. §§ 3402–3408.

188. *Id.* § 3410.

189. *Id.* § 3410(a). The motion or application must include an affidavit or sworn statement from the customer that meets certain requirements, also set out at § 3410(a).

190. *See id.* § 3401(1).

trum, as was demonstrated by the wide variety of participants in a recent proceeding on smart meter data privacy before the Department of Energy.[191] Traditional utilities subject to regulation by state public utilities commissions and federal agencies were a substantial minority of the participants in this proceeding, but a minority nonetheless.[192] As consumers seek applications through which to access, understand, and control their smart meter data, the number of service providers who collect, store, aggregate, analyze, and mine this information will expand dramatically.[193] Legislation that covers only data that is held by utilities, therefore, may be too narrow to protect individual privacy effectively.

2. Proposal Two: Require a Warrant

The second proposed model for smart meter data privacy legislation is based on the recently proposed Geolocation Privacy and Surveillance Act ("GPS Act").[194] The GPS Act restricts intentional interception, disclosure, or use of "geolocation information,"[195] which is defined to be any information "concerning the location of a wireless communication device . . . that, in whole or in part, is generated by or derived from the operation of that device and that could be used to determine or infer information regarding the location of the person."[196] The Act makes a search warrant the "exclusive means of acquiring geolocation information,"[197] except for information acquired in the normal course of business, with consent, in order to respond to

191. DEP'T OF ENERGY, DATA ACCESS AND PRIVACY ISSUES RELATED TO SMART GRID TECHNOLOGIES 25–26 (2010), http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf.

192. *See id.* at B-1.

193. Third parties are vying with utilities to provide the applications that digest smart meter data and present it, repackaged, in a user-friendly form. Google's PowerMeter and Microsoft's Hohm are just two examples. Although PowerMeter and Hohm have been shelved for now, competition is expected to reignite as smart meters enter enough homes to create a robust market. *See The Untimely Demise of PowerMeter and Hohm*, SMARTMETERS.COM (July 8, 2011, 8:13 PM), http://www.smartmeters.com/the-news/2416-the-untimely-demise-of-powermeter-and-hohm.html.

194. Geolocational Privacy and Surveillance Act of 2011, S. 1212, 112th Cong. (2011).

195. *Id.* § (2).

196. *Id.* § 2(a). Importantly, the GPS Act does not define "geolocation information" to be the content of a communication. In Fourth Amendment parlance, "content data," akin to the message inside of an envelope, and "envelope data," which is the addressing information that would appear on the outside of an envelope, are treated differently. *Cf.* Smith v. Maryland, 442 U.S. 735 (1979).

197. Geolocational Privacy and Surveillance Act of 2011, S. 1212, 112th Cong. § 5 (2011).

an emergency or to theft or fraud, or in cases where the information already is configured to be accessible to the general public.[198]

The GPS Act, like the Right to Financial Privacy Act, is designed to protect sensitive information that is received and stored by third parties. It, too, is readily adaptable to smart meter data, although lawmakers applying this framework will again face the challenge of defining the Act's scope. Of the two models discussed here, the GPS Act would initially seem to provide stronger privacy protections because it requires a warrant in almost all cases.[199] Unlike the Right to Financial Privacy Act's highly specific consent requirements,[200] however, the GPS Act does not prescribe language that must be included in a request for a customer's consent to disclose information.[201] Instead, it requires only that consent be "lawful."[202]

If Congress selects the GPS Act as its model for smart meter data privacy legislation, it should limit the Act's warrant requirement exception for information that is intercepted or disclosed based on the customer's consent.[203] When consumers choose to give consent to access their information, the decision often is only partially informed.[204] This is especially true if consent to sharing is required as a prerequisite of receiving service.[205] In a consent-based data sharing system, moreover, the service provider "has an incentive to exaggerate the scope" of the information that it requests in order to maximize the breadth of the consent that it receives.[206] Consent requests that are too narrow also create issues, however, because consumers who must give consent repeatedly to requests that are individually mundane can become desensitized to the choice itself.[207]

---

198. *Id.* § 2. Information arguably should not be considered "accessible" if numbers or code have merely been transformed into a form that can be understood by the average person.

199. *Id.* § 5.

200. The Right to Financial Privacy Act provides:

A customer may authorize disclosure under section 3402(1) of this title if he furnishes to the financial institution and to the Government authority seeking to obtain such disclosure [of his financial records] a signed and dated statement which (1) authorizes such disclosure for a period not in excess of three months; (2) states that the customer may revoke such authorization at any time before the financial records are disclosed; (3) identifies the financial records which are authorized to be disclosed; (4) specifies the purpose for which, and the Government authority to which, such records may be disclosed; and (5) states the customer's rights under this chapter.

12 U.S.C. § 3404 (2006).

201. *See* Geolocational Privacy and Surveillance Act of 2011, S. 1212, 112th Cong. (2011).

202. *Id.* § 2.

203. *Id.*

204. Nicklas Lundblad & Betsy Masiello, *Opt-in Dystopias*, 7 SCRIPTED 155, 165 (2010), http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.pdf.

205. *Id.*

206. *Id*.

207. *Id.*

Congress can mitigate these risks by including language in its smart meter data privacy legislation that requires not merely lawful consent, but some form of "qualifying consent." Qualifying consent could, for example, be defined to require that specific language be contained in the consent request, or limit automatically the amount of time for which a consumer's consent is valid. "Lawful consent" left unelaborated, however, creates perverse incentives that threaten the legislation's underlying goals.

Line drawing is inevitably complicated. Any legislation will require thoughtful debate and careful drafting. The alternative, though, seems to be to wait and wager on the courts. We can leave them to press the limits of analogy, or we can do better.

V. CONCLUSION

Law enforcement access to an individual's smart meter data will test the durability of the "bright line"[208] that the Fourth Amendment has traditionally drawn at the threshold of the home, a barrier by now dismissed by some as merely "a testament to a jurisprudence that has failed to adapt to a reality wherein the four walls of the home no longer demark the boundary between what is kept private and what is not."[209] This data demonstrates why the Supreme Court's interpretation of the third-party doctrine, which has long been accused of doing "great violence"[210] to the Fourth Amendment, is utterly inadequate to protect privacy given recent technological innovations.[211] Some have even declared that the Fourth Amendment is already dead.[212] Securing consumer trust during the deployment of smart meter technology, therefore, may require greater assurance than prognostications about a future Court's ruling can provide.

Which solution, if any, we choose depends, in the end, on the problem we see. True, the warrant requirement is "strong medicine."[213] If our goal is only to prevent bad-faith harassment by law enforcement, perhaps the protections of the first proposal are enough. If we think of privacy as something more fundamental, however, we should take the stronger dose. Whatever our choice, we must act.

---

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

209. Doran, *supra* note 15, at 918.

210. LAFAVE, *supra* note 103, at 747.

211. *Cf.* J. Choper, Y. Kamisar & L. Tribe, 1 THE SUPREME COURT: TRENDS AND DEVELOPMENTS 143–44 (1979) ("It is beginning to look as if the only way someone living in our society can avoid 'assuming the risk' that various intermediary institutions will reveal information to the police is by engaging in drastic discipline, the kind of discipline characteristic of life under totalitarian regimes.").

212. Kozinski & Grace, *supra* note 151.

213. *See* Kerr, *supra* note 101, at 590.