# Privacy Implications of Smart Meters

By Cheryl Dancey Balough

Balough Law Offices, LLC
Chicago, Illinois

First published in *Chicago-Kent Law Review,* Vol. 86, Issue 1 (2011)

# PRIVACY IMPLICATIONS OF SMART METERS

CHERYL DANCEY BALOUGH*

## INTRODUCTION

It's 1984, Orwellian time. The telescreens are everywhere, monitoring the intimate details of citizens' lives within their own homes. Big Brother is watching you. Now transport yourself to 2010. Smart meters—along with other smart devices—are being installed in homes across the country. By measuring energy consumption by appliance every fifteen minutes, they capture details on how you spend your days and nights. When you turn off the lights. When you take a shower. When you leave home. Where your electric vehicle is being charged. But who is watching you? Who has access to all this information? The electric company? Appliance manufacturers? The government? The Internet? What might they do with it? Orwell's 1984 has not come to pass, but smart meters have. This article examines the privacy implications of smart meters and explores options for protecting one of our most basic rights.

## I. A RECENT HISTORY

On October 27, 2009, the President of the United States announced $3.4 billion in Smart Grid Investment Grant awards—the largest group of American Reinvestment and Recovery Act awards ever made in a single day.[1] More than one hundred companies, utilities, municipalities, and other entities in forty-two U.S. states, the District of Columbia, and Guam received the awards, with a sizeable portion going toward expanding access to smart meters and associated smart appliances and devices.[2] Smart me-

* Cheryl Dancey Balough is a member of Balough Law Offices, LLC, a firm that focuses on public utility, privacy, and intellectual property law. She can be contacted at cbalough@balough.com. The author wishes to thank Chicago-Kent College of Law Professor Fred P. Bosselman, for his critique of the author's initial exploration of privacy issues raised by the implementation of smart meters, and Richard C. Balough, for his valuable insights and editorial recommendations.

1. Press Release, U.S. Dep't of Energy, President Obama Announces $3.4 Billion Investment to Spur Transition to Smart Energy Grid (October 27, 2009) (on file with author), *available at* http://www.energy.gov/news2009/8216.htm.

2. *Id*; U.S. Dep't of Energy, *Recovery Act Selections For Smart Grid Investment Grant Awards - By State*, available at http://www.energy.gov/recovery/smartgrid_maps/SGIGSelections_State.pdf (last visited Oct. 15, 2010)

ters, which are digital meters that offer "two-way, near real time communication" between the home and the electric utility, are a crucial component of a smart grid.[3] As of mid-2009, one research firm estimated that smart meters represented six percent, or 8.3 million, of all electric meters operating in the country.[4] The U.S. Department of Energy projects that fifty-two million more will be installed by 2012.[5] In conjunction with smart appliances, data management software, other smart devices like programmable communicating thermostats (PCTs), and home area networks (HANs), the smart meters promise to provide utilities, electricity consumers, and possibly others with rich data on electricity consumption by appliance or type of use in thirty or fifteen-minute intervals.[6] Their goal is to help improve energy efficiency based on the assumption that customers will adjust their consumption patterns (or allow the utility to do so) if they are properly informed with near real-time detailed information about their own electricity consumption, its cost, and comparisons to neighbors' consumption levels while simultaneously receiving education on simple, concrete steps they can take to reduce their electricity bills by adjusting those usage patterns.[7]

As the rush to install residential smart meters accelerates, some privacy experts, utilities, and governmental agencies are calling for caution until the privacy implications of smart meters can be addressed. Jules Polonetsky, director of the Future of Privacy Forum, emphasizes that many utilities are "worried about fulfilling basic operational concerns and getting meters installed and [saying], 'Well, when there's a regulator or rule I'll worry about complying with that,' or 'when I actually want to make more use of the data. Today I just want to get the meter installed.'"[8] The ability to get rich data from the smart meters, however, might also just be the

3. *Frequently Asked Questions*, SMART GRID CITY, http://smartgridcity.xcelenergy.com/learn/frequently-asked-questions.asp (last visited July 29, 2010).

4. *More than 8 Million Smart Meters installed in US*, July 21, 2009, Parks Associates, http://www.parksassociates.com/press/cited/Smart_Meters.html.

5. U.S. DEP'T OF ENERGY, SMART GRID SYSTEM REPORT, at vi (July 2009), *available at* http://www.oe.energy.gov/DocumentsandMedia/SGSRMain_090707_lowres.pdf.

6. Jules Polonetsky, Privacy and the Smart Grid: New Frontiers, New Challenges, Presentation at Privacy by Design: The Definitive Workshop, at 8 (November 2009) (on file with author), *available at* http://www.privacybydesign.ca/madrid09/Smart_Grid_Privacy_Madrid_PowerPoint_JP_Final.pdf.

7. *See* Press Release, Am. Council for an Energy-Efficient Econ., ACEEE Study Finds "Smart Meters" Not Smart Enough to Slash Residential Power Use and Significantly Reduce Consumer Electric Bills (June 29, 2010) (on file with author), *available at* http://www.aceee.org/press/e105pr.htm; Lisa Wood, Consumers Are the Key to Future Smart Energy Management 8-10, Presentation to the Eastern New Mexico State University Center for Public Utilities Current Issues 2010 conference (March 16, 2010) (on file with author), *available at* http://www.edisonfoundation.net/iee/IssueBriefs/Wood_SantaFe_March10.pdf.

8. *Smart Grid Elevated to Top Issue by Leading Privacy Watchdogs*, SMART GRID TODAY (Dec. 17, 2009), http://www.smartgridtoday.com/members/1060print.cfm.

smart grid's Achilles' heel.[9] If homeowners fear that installation of smart meters will compromise their privacy, a backlash could arise that would stall the adoption of this promising technology along with residential participation in the smart grid.[10] "[L]ack of consumer confidence in the security and privacy of their energy consumption data" could also result in litigalitigation.[11] As Elias Quinn, a Colorado Supreme Court clerk who helped Colorado's Public Utility Commission (COPUC) conduct informational hearings on smart grid policy, stated, "Get one really salient privacy invasion that makes the front page of the *New York Times* and the *Washington Post* and you'll bring to a dead stop smart grid development."[12]

Not all players in the smart grid industry believe that installation of smart meters should slow down pending resolution of privacy concerns; nonetheless, widespread concern about privacy risks associated with the devices exists.[13] As part of its responsibility to develop standards for the smart grid, the National Institute of Standards and Technology (NIST) established a Cyber Security Working Group within a new Smart Grid Interoperability Panel (SGIP-CSWG) with members from the "private sector . . ., academia, regulatory organizations, and federal agencies."[14] NIST and the privacy subgroup of the SGIP-CSWG conducted a privacy impact assessment, and in September 2009, NIST issued the first draft of its *Smart Grid Cyber Security Strategy and Requirements* interagency report.[15] The volume of comments submitted to NIST in response to the first draft manifest the widespread concern about privacy risks associated with smart meters. The Electronic Privacy Information Center, The Center for Democracy & Technology, and thirty-three other privacy groups, utilities, technology firms, and other entities involved in the burgeoning smart grid industry filed more than 450 comments.[16]

---

9. Polonetsky, *supra* note 6, at 3.

10. NAT'L INST. OF STANDARDS AND TECH., SMART GRID CYBER SECURITY STRATEGY AND REQUIREMENTS, DRAFT 1 - COMMENT RESOLUTION 123, http://csrc.nist.gov/publications/drafts/nistir-7628/nistir7628draft1_commentdisposition.pdf; *see also* PUBLIC SERVICE COMPANY OF COLORADO, INITIAL COMMENTS IN RESPONSE TO DECISION NO. C09-0878, at 4, *available at* https://www.dora.state.co.us/pls/efi/EFI.Show_Filing?p_session_id=&p_fil=G_12903.

11. NAT'L INST. OF STANDARDS AND TECH., SMART GRID CYBER SECURITY STRATEGY AND REQUIREMENTS, DRAFT 2 at 111 (February 2010) (on file with the law review).

12. *Smart Grid Elevated to Top Issue by Leading Privacy Watchdogs*, *supra* note 8.

13. *See* NAT'L INST. OF STANDARDS AND TECH., *supra* note 10.

14. NAT'L INST. OF STANDARDS AND TECH., *supra* note 11, at 1.

15. *Id.* at 102; NAT'L INST. OF STANDARDS AND TECH, *supra* note 10, at 1.

16. Press Release, Nat'l Inst. of Standards and Tech., NIST Released the Second Draft of NIST Interagency Report (NISTIR) 7628 **(**February 2, 2010) (on file with author), *available at* http://csrc.nist.gov/news_events/index.html.

This vigorous reaction should not be a surprise. The past forty years have seen a strong interest in controlling the collection and use of personal information. In 1973, the U.S. Department of Health, Education, and Welfare issued its *Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, the result of the committee's study on recordkeeping in the "computer age."[17] That report, which became commonly known as the "HEW Report," advocated "fair information practices" and formed much of the basis for the Privacy Act of 1974.[18] In the ensuing thirty-five years, Congress passed several laws to protect information privacy, including the Computer Fraud and Abuse Act (18 USCS § 1030), the Electronic Communications Privacy Act of 1986 (18 USC §§ 2510–2522, 2701–2709), the Driver's Privacy Protection Act of 1994 (18 USC §§ 2721–2725), the Health Insurance Portability and Accountability Act of 1996 (P.L.104–191), and the Gramm-Leach-Bliley Act of 1999 (15 USC §§ 6801–6809). More recently, the media have reported frequently on concerns of the general public about privacy on the Internet, including how employers increasingly use voluntary posts on social media sites like Facebook and LinkedIn to make both hiring and termination decisions.[19] Social media users themselves revolted when Facebook loosened its privacy controls in December 2009 and made its users' profiles more accessible to the public, forcing the company into a partial retreat a few months later.[20]

Now, privacy advocates, governmental agencies, utilities, and third parties poised to benefit from the smart grid are struggling over how best to address the threats to privacy inherent in smart meters. Three factors fuel the concern of those advocating for additional, specific measures that will protect privacy compromised by the installation of smart meters. First, the wealth of information that smart meters and affiliated appliances and devices make available can threaten both consumers' privacy within their homes and their ability to control the distribution of their personal information outside the home. Second, as necessary consumers of electricity, people do not have other options. Third, despite the multiple information

17. U.S. DEP'T OF HEALTH, EDUC., AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (July 1973).

18. Robert Gellman, *Fair Information Practices: A Basic History* BOBGELLMAN.COM (May 13, 2010), available online at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

19. Press Release, Proofpoint, Proofpoint Survey Says: State of Economy Leads to Increased Data Loss Risk for Large Companies (August 10, 2009) (on file with author), *available at* http://www.proofpoint.com/news-and-events/press-releases/pressdetail.php?PressReleaseID=245.

20. Caroline McCarthy, *Do Facebook's New Privacy Settings Let It Off the Hook?*, CNET NEWS (May 26, 2010), http://news.cnet.com/8301-13577_3-20006054-36.html.

privacy laws passed in the past few decades, none of them adequately address the new challenges to privacy posed by smart meters.

## II. TYPES OF THREATS TO PRIVACY PRESENTED BY SMART METERS

Legal scholars have proposed various concepts of privacy over the past 120 years or so, and the country's founding fathers certainly contemplated privacy rights when drafting the Bill of Rights. A discussion of those concepts and their origins is beyond the scope of this article. It is important to note, however, that the threats to privacy connected to smart meters lie primarily within the concepts of a right to be left alone within one's home and the right to control personal information. The first right is embedded in the Fourth Amendment of the U.S. Constitution:

> The right of the people to be secure in their person, 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 persons or things to be seized.[21]

The second right—to exercise control over the disclosure of personal information—has been discussed by a number of legal scholars.[22] The U.S. Supreme Court also recognized this right in 1977 in *Whalen v. Roe*.[23]

Smart meters can compromise both of these rights. Many smart meters are found within residences, and all of the meters, even those that are not located within in the home itself but adjacent to an outside wall of the house or somewhere on the home's property, record information about what transpires within the home. Before smart meters, the only information that utilities gathered from electric meters was the total consumption of electricity on a monthly or less frequent basis as measured by kilowatt hours.[24] With the new smart meters, it is not clear which and how much information will eventually be gathered. Because each smart meter is associated with a unique street address, however, data sent from the meter is

---

21. U.S. CONST. amend. IV.

22. *See* ADAM CARLYLE BRECKENRIDGE, THE RIGHT TO PRIVACY (1970); ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); RANDALL P. BEZANSON, THE RIGHT TO PRIVACY REVISITED: PRIVACY, NEWS, AND SOCIAL CHANGE, 1890-1990, 80 CALIF. L. REV. 1133 (1992).

23. In *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977), the Court recognized the "individual interest in avoiding disclosure of personal matters," although it found there that the statute at issue did not "pose a sufficiently grievous threat" to that interest.

24. Some jurisdictions require the electric utility to read residential meters each month; other jurisdictions permit the utility to send estimated monthly bills with actual meter readings occurring less frequently.

personally identifiable.[25] All smart meters permit the electric utility to remotely monitor electricity consumption not just monthly—but on a real-time or near real-time basis.[26] Depending on the meter, this is at least as frequently as hourly and often as frequently as every fifteen minutes, with some meters measuring usage in five minute intervals.[27]

The real-time monitoring can also occur by room, by appliance, and potentially by outlet—depending on the types of appliances in the home and the additional devices that form part of the HAN—and it is estimated that the monitoring for an average home will generate between 750 and 3,000 data points per month.[28] Because appliances (including heating and cooling systems, refrigerators, toasters, hair dryers, computers, and home entertainment centers) account for sixty to ninety percent of residential energy usage, managing their energy consumption can greatly impact the energy load at any time of day.[29] Manufacturers have begun to make more and more of these appliances grid-enabled—that is, smart appliances—by enabling them to communicate with smart meters. The appliances continually send their energy usage, labeled as consumed by that appliance, to the smart meter. The smart meter reads that communication from all smart appliances and can generate a load signature for each home.[30] A resident can then view the home's detailed energy usage on an in-home display (although there might be an additional charge for this) or on the electric utility's secure website using unique login information and make informed decisions on how to adjust energy usage.[31] The resident or electric company can relay instructions to the smart appliances either manually or auto-

25. NAT'L INST. OF STANDARDS AND TECH., NIST FRAMEWORK AND ROADMAP FOR SMART GRID INTEROPERABILITY STANDARDS, RELEASE 1.0, at 38, available at http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

26. *OE Recovery Act - Frequently Asked Questions*, U.S. DEP'T OF ENERGY, http://www.oe.energy.gov/recovery/1225.htm (last visited July 29, 2010); *see also* Frank Hoss, *Smart Grid Data Management: 7 Tips from the Trenches*, SMARTGRIDNEWS.COM (June 2, 2010), http://www.smartgridnews.com/artman/publish/Business_Strategy_Resources/Smart-Meter-Data-Management-7-Essential-Tips-from-the-Trenches-2445.html.

27. *See Auburn, Indiana, picks 5-minute intervals for use reporting*, SMARTGRIDTODAY, (December 23, 2009), http://www.smartgridtoday.com/public/1079.cfm?sd=35; *Frequently Asked Questions*, SMART GRID CITY, http://smartgridcity.xcelenergy.com/learn/frequently-asked-questions.asp (last visited Oct. 15, 2010); *Frequently Asked Questions*, SMART METER TEXAS, https://www.smartmetertexas.com/CAP/public/learn_more/learn_more_faq.html.

28. NAT'L INST. OF STANDARDS AND TECH., *supra* note 10, at 43.

29. *End Use: Appliances*, SMARTGRIDNEWS.COM, http://www.smartgridnews.com/artman/publish/End_Use_Appliances/ (last visited July 30, 2010).

30. Lillie Coney, Privacy and the Smart Grid: How to Address Consumer Concerns without Jeopardizing the Growth of the Grid, Presentation at Smart Grid Summit, at 8-9 (April 13, 2010) (on file with author), *available at* http://epic.org/privacy/smartgrid/EPIC_Statement_Smart_Grid_Summit_Cybersecurity_and_Privacy.pdf.

31. Smart Grid City, *supra* note 27; Smart Meter Texas, *supra* note 27.

matically based on a pre-established algorithm to the smart meter.[32] In addition, anyone with access to a resident's display or the website could review the load signature to determine what time the person arrives and leaves home, if the security system is activated, if one cooks with a microwave or the stove, the presence of certain medical equipment, how much and when the household watches television, if someone gets up in the middle of the night and uses the computer, which equipment is left on 24/7, etc.[33]

The energy consumption of a plug-in hybrid electric vehicle (PHEV) could also be monitored by the smart meter. Because each PHEV likely will be "registered" to a home electric account, smart meter data would show when and how much a person's vehicle is charged, as well as where it is charged.[34] If someone visits a friend and charges his PHEV there, the friend's smart meter log would show when the visitor's car was there and for how long it was charged.[35] By compiling information from various smart meters, one could reconstruct a person's travel habits.

Utilities have also begun to encourage residential customers with smart meters to install home energy management systems (EMS).[36] The home EMS connects to the smart meter and is designed to enable a customer to manage the HAN, which consists of smart appliances, PCTs, intelligent sockets, in-home displays, and other smart in-home devices.[37] While many of these systems and devices are still in their infancy, programs like the Smart Grid Investment Grant awards are accelerating their development. Near real-time data on people's activities within their homes—information that has never before been available to people other than those in the home—is quickly becoming available.[38] Because myriad other systems that will interact with smart meters have yet to be designed, one cannot fully predict the types and amounts of personally identifiable information that will be monitored or collected.[39] Utilities might argue that

32. *Smart Meter Texas*, *supra* note 27; *see also* NAT'L INST. OF STANDARDS AND TECH., *supra* note 11, at 33.

33. Polonetsky, *supra* note 6, at 8-10.

34. William Levis, Smart Privacy for a Smart Grid at 9, Smart Grid Today Web Conference (April 13, 2010) (on file with author); *see also NIST Framework*, *supra* note 25, at 35.

35. Levis, *supra* note 34, at 9.

36. Smart Meter Texas, *supra* note 27; *see also* NAT'L INST. OF STANDARDS AND TECH., *supra* note 11, at 22.

37. NAT'L INST. OF STANDARDS AND TECH., *supra* note 11, at 22, 44; *see also* Press Release, Cisco, Cisco Powers up Energy Management Tools for Utilities, Consumers, Businesses, (June 29, 2010) (on file with author), *available at* http://newsroom.cisco.com/dlls/2010/prod_062910c.html?print=true; NAT'L INST. OF STANDARDS AND TECH., *supra* note 10, at 64.

38. Coney, *supra* note 30, at 9-10.

39. Levis, *supra* note 34, at 20.

the monitoring of detailed data captured through the smart meters does not present great cause for concern because utilities have both privacy policies and staff in place to address security issues. The sheer volume and types of personal data to be collected by smart meters, however, are far more threatening to privacy than how much energy a household consumes on a monthly basis, and the security issues themselves are different. Furthermore, as Polonetsky points out, security is not synonymous with privacy.[40]

That is not to say that security is not an issue for those concerned about privacy risks associated with smart meters. NIST, which was charged with developing national standards for the smart grid, treats privacy as a component of what it views as the much larger issue—cyber security.[41] Utilities are using the Internet and public networks for transfer of smart meter data.[42] There is a strong push to increase the use of commercial broadband, instead of utility-owned wires, for the transfer of smart meter data back to the utilities.[43] Right now, residents in states like California and Texas, where the smart meter rollout has been underway for a couple of years, must access utility websites to view data generated by their own smart meters.[44] Whenever personal information is accessible on the Internet, there is a concern about privacy because of breaches in security. Hackers and unauthorized users could use the wealth of smart meter personal data to enable crimes like identity theft, burglary, vandalism, stalking, and domestic abuse.[45] Even if residents can access their smart meter data via the in-home display of a home EMS, with the data relayed to the utility on utility-owned wires, the HANs will rely on wireless technology given its low cost compared to wires, making the data vulnerable.[46] Cryptographic and physical controls, while certainly a deterrent to unauthorized access, are not foolproof mechanisms to war driving, man-in-the-middle attacks, and impersonators.[47] At a security conference in 2009, one security consul-

40. *Privacy Advocate Details Weaknesses in Smart Grid, Utility Leadership*, SMARTGRIDTODAY (March 10, 2010), http://www.smartgridtoday.com/members/1338print.cfm.

41. NAT'L INST. OF STANDARDS AND TECH., *supra* note 11, at 5.

42. NAT'L INST. OF STANDARDS AND TECH., *supra* note 10, at 20.

43. *FCC Broadband Plan Urges New Energy Data Policies at FERC, DOE*, SMARTGRIDTODAY (March 17, 2010), http://www.smartgridtoday.com/members/1363print.cfm.

44. Smart Grid City, *supra* note 27; Smart Meter Texas, *supra* note 27.

45. NAT'L INST. OF STANDARDS AND TECH., *supra* note 10, at 19.

46. *Id.* at 38; *see also 2010 Smart Grid Industry Survey: Executive Summary*, AVIAT NETWORKS, www.portals.aviatnetworks.com/exLink.asp?8884441OV23D86I36231748 (on file with author) (noting that "[s]urvey results indicate that wireless technologies are considered very important elements of Smart Grid programs").

47. NAT'L INST. OF STANDARDS AND TECH., *supra* note 10, at 38.

tant demonstrated how he and his team could use a worm to take over the smart meters in 15,000 out of 22,000 homes within twenty-four hours.[48]

Assuming the risks of criminal attacks could be made negligible through enhanced cyber-security, authorized access to the smart meter data also poses threats. Utilities themselves could pose a threat to the privacy of the data. In the past, only those utility employees with access to certain components of billing data could see confidential information about customers, but the unprecedented volume of personal user data emerging from the smart meters is of great value to myriad utility employees charged with monitoring and maintaining the smart grid and managing electricity consumption. Electric utilities will need new policies and procedures concerning personnel hiring and training, more complex access and authorization algorithms, and greatly enhanced privacy policies to minimize the possibility of intentional and inadvertent disclosures of personal data.[49] Additionally, electric utilities are already distributing energy usage comparisons to customers.[50] Current utility mechanisms to protect privacy are not sufficient.

Electric utilities have begun struggling to determine which third party vendors should have access to smart meter data and the extent to which the utilities can control what third party vendors do with the data. Companies that manufacturer home EMS and in-home display systems are actively marketing their products to utilities for distribution to the electric company's residential customers.[51] These vendors include companies that traditionally rely on a business-to-business sales model, like Cisco, OPower and General Electric, as well as companies that have had great success selling to end users, like Google and Microsoft.[52] The latter two companies are using a push-pull marketing strategy to promote their Google PowerMeter and Microsoft Hohm systems to residential end users, while also completing sales directly to electric utilities. The relationships between the home EMS manufacturers, utilities, and other third parties that offer complemen-

48. Katie Fehrenbacher, *Smart Meter Worm Could Spread like a Virus*, GIGAOM (July 31, 2009), http://gigaom.com/cleantech/smart-meter-worm-could-spread-like-a-virus/ (on file with author).

49. NAT'L INST. OF STANDARDS AND TECH., *supra* note 11, at 8, App. C.

50. Julie Wernau, *ComEd to Sample Power by the Hour*, CHI. TRIB., June 21, 2010 (News), at 19, 21.

51. *New Cisco Offerings Focus on the Home*, SMARTGRIDTODAY (June 30, 2010), http://www.smartgridtoday.com/public/1762print.cfm; *see also* Jeff St. John, *Microsoft Hohm: First Seattle City Light, Now Xcel Energy*, GREEN LIGHT (November 12, 2009), http://greentechmedia.com/green-light/post/microsoft-hohm-first-seattle-city-light-now-xcel-energy/.

52. *See* St. John, *supra* note 51; GOOGLE POWERMETER, http://www.google.com/powermeter/about/ (last visited July 29, 2010); *OPower's 3.0 Upgrade Gives Utility Customers Data They Can Actually Use*, SMARTGRIDTODAY (February 12, 2010), http://www.smartgridtoday.com/members/1248print.cfm.

tary devices and systems are becoming increasingly complex with smart meter data flowing back and forth between the companies.[53] This data transfer is occurring even before comprehensive privacy policies are in place.

Once the data reaches a third party's servers, the third party typically has control over how it uses and shares that data. Microsoft Hohm, for example, allows the general public to click on a specific house on a map and see the electric usage for that house.[54] At this point, the energy usage data shared is at a high level and Microsoft's privacy statement asserts that it will not disclose an end user's personal data outside of the Microsoft family of subsidiaries, affiliates, and companies with whom it co-brands without the user's consent.[55] That family is quite large and difficult to discern for the general public, and Microsoft can always change its privacy statement. Furthermore, the companies that co-brand with home EMS providers could include a host of companies that wish to market their products directly to residents with smart meters.[56] These companies are confident that "they can make a profit in the smart grid information area but their business models will rely on getting" smart meter data.[57] While some consumers might appreciate this service in the same way that they enjoy suggestions for additional purchases from Amazon.com, Netflix, or Tivo, other consumers will find yet more unsolicited advertising burdensome and invasive—especially when they did not give the marketers permission to solicit them. This invasion is likely to occur because some third party companies having strong involvement with smart devices for the homes have not even formed privacy policies or communicated them to end users. For example, the chief executive officer of OPower, a smart grid and energy efficiency software company that works with twenty-six utilities, states that he has not yet had to deal with privacy concerns, adding that "[t]he way we've anticipated dealing with them is to opt-out customers who are unhappy with the analysis."[58]

Electric utilities not only lack the ability to control the privacy policies and procedures of third parties with whom they affiliate, but they also cannot control access to smart meter data at cu stomers' homes. In the case of

53. *See* St. John, *supra* note 51.

54. *See* MICROSOFT HOHM BETA, http://www.microsoft-hohm.com/ (last visited August 1, 2010).

55. Microsoft Online Privacy Statement, MICROSOFT, http://privacy.microsoft.com/en-us/fullnotice.mspx#EWB (last updated August 2010).

56. Leslie Harris, *Smart Grid: Classic Struggle of Reward vs. Risk*, HUFFINGTON POST, (December 10, 2009), http://www.huffingtonpost.com/leslie-harris/smart-grid-classic-strugg_b_387446.html.

57. *Privacy Advocates Describe Pros, Cons of Consent to Use Meter Data*, SMARTGRIDTODAY, (December 18, 2009), http://www.smartgridtoday.com/members/1064print.cfm.

58. *OPower's 3.0 Upgrade Gives Utility Customers Data They Can Actually Use*, *supra* note 52.

smart meters installed in buildings with multiple dwelling units, landlords and subsequent renters or tenants might be able to access another resident's smart meter data.[59] If smart meters are not wiped clean of data between tenants, a subsequent tenant could view the previous tenant's personal data. A landlord could also access the data and use it to claim that a tenant is in violation of a lease.

Other third parties might seek to obtain smart meter data from the residential end user directly as a precondition to signing a contract or via discovery in a legal dispute. Appliance manufacturers could determine usage patterns for their appliances and use that data to invalidate warranties.[60] Similarly, car manufacturers would find the data helpful in resolving warranty claims. Health insurance companies could want access to determine if an insured party has an unhealthy lifestyle.[61] Financial institutions might find it beneficial to know if a potential mortgagor is living full-time at a location.[62] Divorce attorneys might want to use the data to discredit the opposing party in any number of ways, for example, by showing repeated premarital visits to a lover.

Law enforcement officials constitute yet another group that will want access to smart meter data. In fact, in some areas of the country, law enforcement agencies have already used energy consumption data as part of an early investigational tool into potential illegal activities. In Texas, a police detective allegedly used Austin Energy to help data-mine energy usage to identify possible residential marijuana growing operations.[63] In California, law enforcement officers obtained a search warrant based solely on an unusually high electric bill to access a family's house in search of evidence of marijuana production.[64] It turned out that the family in question simply used a lot of energy.[65] In both cases, the alleged data-mining focused on overall electricity consumption in excess of average. Smart meter data would allow for much more focused investigations because consumption could potentially be tracked by appliance and time of day. Use of smart meter data could help law enforcement solve crimes, of

59. NAT'L INST. OF STANDARDS AND TECH., *supra* note 10, at 203.

60. NAT'L INST. OF STANDARDS AND TECH., *supra* note 11, at 112-13; *see also* Rebecca Herold, *Smart Grid Privacy Concerns*, REBECCA HEROLD & ASSOCIATES (October 2009)http://www.privacyguidance.com/files/SmartGrid_PrivacyHeroldOct2009.pdf.

61. NAT'L INST. OF STANDARDS AND TECH., *supra* note 10, at 55; *see also* Herold, *supra* note 60.

62. NAT'L INST. OF STANDARDS AND TECH., *supra* note 10, at 55.

63. Jordan Smith, *APD Pot-Hunters Are Data-Mining at AE*, AUSTIN CHRONICLE, November 16, 2007, *available at* http://www.austinchronicle.com/gyrobase/Issue/story?oid=oid%3A561535

64. *A Suspicious Electric Utility Bill?*, PRIVACY.ORG (March 28, 2004), http://privacy.org/archives/001250.html.

65. *Id.*

course. One could also argue that there would likely be only a few isolated instances of misuse. On the other hand, there is a history of voluntary utility compliance with government requests to share personal consumer usage information, such as by the phone companies after 9/11.[66]

Even if electric utilities do not voluntarily disclose detailed personal consumption from smart meters to law enforcement, the government may force the disclosure. In early 2010, the U.S. Department of Justice asserted in federal court that no constitutional bar exists to law enforcement obtaining cell phone records from communication service providers, arguing that "[t]he government is not required to use a warrant when it uses a tracking device."[67] The Department asserted that law enforcement needs only a 2703(d) order, which requires that the records are "relevant and material to an ongoing criminal investigation."[68] The U.S. Supreme Court has held, however, that the warrantless monitoring of a beeper *inside* a house violates the Fourth Amendment.[69] Smart meter data, which "tracks" energy usage, is generated inside the house but conveyed to the electric utility, so whether or not law enforcement may monitor it as a "tracking device" without a search warrant is unclear. Concerns about the privacy implications of law enforcement access to smart grid meter are real and suggest the need for strong Fourth Amendment protections.[70]

Given the value of smart meter data to a variety of groups, as detailed above, residential electricity consumers are justifiably concerned about the lack of control over personal information that smart meter installation presents. Some argue that clarification about who owns the data might put these concerns to rest. Reaching that clarification will not be simple. In the February 19, 2010, issue of the *Federal Register*, the executive branch's Office of Science and Technology Policy requested public comment on the first release of a smart grid interoperability framework document issued by NIST.[71] The request encouraged potential responders to answer several specific questions, including: "Who owns the home energy usage data? Should individual consumers and their authorized third-party service pro-

66. *In re: National Security Agency Telecomm. Records Litigation*, 630 F. Supp. 2d 1092 (N.D. Cal. 2009); *see also* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, *available at* http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

67. Declan McCullagh, *Justice Dept. Defends Warrantless Cell Phone Tracking*, CNET NEWS (February 13, 2010), http://news.cnet.com/8301-13578_3-10453214-38.html.

68. *Id.*

69. United States v. Karo, 468 U.S. 705, 714 (1984).

70. NAT'L INST. OF STANDARDS AND TECH., *supra* note 10, at 55-56.

71. Consumer Interface with the Smart Grid, 75 Fed. Reg. 7526-28 (2010).

viders have the right to access energy usage data directly from the meter?"[72]

No consensus exists regarding smart meter data ownership. Some parties take the position that the individual energy consumer owns the data. For example, the Texas Utilities Code states that "[a]ll meter data, including all data generated, provided, or otherwise made available, by advanced meters and meter information networks, shall belong to a customer, including data used to calculate charges for service, historical load data, and any other proprietary customer information."[73] NIST, on the other hand, states that utilities own the data generated by the smart meters analogous to a car rental company's ownership of data regarding car rentals.[74] NIST also points out that, even if the consumer were to own the smart meter data, disputes as to the true consumer's identity may arise. Both a home owner and a renter of the home could claim ownership of the usage data.[75] Some utilities argue that they have at least some ownership rights in the data. One California utility, for example, argues that, while the customer possesses the right to decide if he wants to release his smart meter data to a third party, the utility would be due "some consideration" at that point the data is released.[76] The Public Service Company of Colorado believes that "the energy usage information should be viewed as the property of the utility" and that the COPUC must provide the utility with a mechanism for recovering the costs associated with disclosure of customer data to third parties upon the customer's written request.[77] Senator Mark Udall's proposed amendment to the Public Utility Regulatory Policies Act of 1978, S. 3487, states that electric consumers have a right to access smart meter data and "retain the privacy of [their] electric energy information," but does not address the issue of data ownership.[78]Even a resolution to the ownership controversy in favor of the consumer, however, does not ensure control over personal data. Were consumers to own the smart meter data and have the power to authorize or refuse disclosure to third parties, the data remains subject to security breaches, inadvertent disclosure by the utility, and unknowingly authorized releases by the consumer to third parties—all of which would result in personal data reaching possibly unsecured areas on

72. *Id.* at 7527.

73. Tex. Utilities Code § 39.107(b).

74. NAT'L INST. OF STANDARDS AND TECH., *supra* note 11, at 114.

75. *Id.*

76. *Burbank Municipal Utility Manger Tackles Issue*, SMARTGRIDTODAY (September 21, 2009), http://www.smartgridtoday.com/members/755print.cfm.

77. PUBLIC SERVICE COMPANY OF COLORADO, *supra* note 10, at 12.

78. S. 3487, 111th Cong. § 2 (2010); *see also* H. R. 4860, 111th Cong. § 215 (2010) (a companion bill in the House advanced by Representative Edward Markey).

the Internet, where it might reside permanently. As George Washington University law professor Jeffrey Rosen recently stated that "the permanent memory bank of the Web increasingly means there are *no* second chances."[79] Rosen noted that a group of experts in technology, the law, and cyberspace are currently exploring options for "recreating the possibility of digital forgetting," but for now personal data that finds its way to unsecured areas of the Internet will be beyond the data owner's control and forever accessible to the general public.[80]

Control over personal data might also be lost through the aggregation of non-personal data with publicly available data. A recent study conducted at Carnegie Mellon University demonstrated how one can predict individuals' social security numbers within very narrow ranges using only public data.[81] A variation on the phenomenon of obtaining personal data by aggregating non-personal and public data is "trail identification." Experts have shown that, by using algorithms, one can learn an individual's identity "from the trails of seemingly anonymous" data that they leave behind when they visit the Internet.[82] In relation to smart meters, participants in the NIST Cyber Security Working Group express a strong concern that combining publicly available personal information with seemingly anonymous smart meter data elements might reveal personal, undisclosed lifestyle information.[83] For example, Google could use smart meter data obtained from its PowerMeters with information obtained from Google's other Internet ventures to generate powerful personal information about PowerMeter users.[84]

## III. LACK OF CONSUMER OPTIONS

One solution to these myriad threats to privacy might be to simply refuse to allow smart meter installation in your home, but electric consumers have no truly viable options. With the exception of a very few who have chosen to live outside the mainstream of American life, we rely on electricity in this country. We need it to light our homes, to utilize heating and air conditioning, to run our computers, to run our microwaves, to enjoy our

79. Jeffrey Rosen, *The End of Forgetting*, N.Y. TIMES MAGAZINE, July 25, 2010, at 32.

80. *Id.* at 34.

81. Alessandro Acquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 PROC. NAT'L. ACAD. SCI. 10975-80, *available at* www.pnas.org/cgi/doi/10.1073/pnas.0904891106.

82. Bradley Malin, Latanya Sweeney, & Elaine Newton, *Trail Re-identification: Learning Who You Are from Where You Have Been*, CARNEGIE MELLON DATA PRIVACY LAB (Data Privacy Lab. Tech. Report, Pittsburgh),(March 2003), http://privacy.cs.cmu.edu/dataprivacy/projects/trails/trails1.pdf.

83. NAT'L INST. OF STANDARDS AND TECH., *supra* note 11, at 110.

84. Coney, *supra* note 30, at 11-12.

televisions and entertainment centers, and to recharge our cell phones. We cannot imagine life without it—except for the recreational or educational trip to a community that reflects the realities of life before electricity became widely available. As electric utilities receive permission from their state public utility commissions to replace traditional meters with smart meters and expand their rollout, the utilities will cease servicing traditional meters and consumers will need to permit the installation of a smart meter in their homes if they want to continue to receive electricity.[85] Unlike cell phones or credit cards, consumers cannot opt out of the technology or decide which smart meter to have installed.

The notice and consent model employed to let consumers know what happens with the data from their smart meters also severely limits or nullifies options. Once a smart meter is installed and consumers are asked to set up an online account for secure access to data from the smart meter, they will typically need to "click" their consent to an agreement. That agreement might contain a utility's "terms and conditions" and privacy statement, including information on the utility's procedures for and the consumer's consent to disclosure of smart meter data.[86] Lillie Coney, associate director of the Electronic Privacy Information Center (EPIC), noted in comments before the U.S. House Committee on Science and Technology that studies indicate that people do not read agreements, privacy statements, or other disclaimers before downloading or activating Internet programs.[87] In fact, the majority of people mistakenly believe that the presence of a privacy statement automatically means that their privacy is protected.[88] Another study conducted for the Privacy Leadership Initiative found that the vast majority of people do not read or only glance at privacy notices sent to them.[89] In the case of a click-through agreement for one's own smart meter, consumers will likely feel that they have no choice because they need electricity. As Coney pointed out, "You're talking about my ability to get electricity. . . . If I don't consent to it, the utility may not give me power? That's a very scary choice."[90] While debate continues over the adequacy of the notice and consent model, NIST appears inclined to recommend that

85. *Residents Express Concern over SmartMeter Radiation*, KGO-TV (July 29, 2010), http://abclocal.go.com/kgo/story?section=news/business&id=7583605.

86. *See, e.g.*, Smart Grid City, *supra* note 3; Smart Grid Texas, *supra* note 27.

87. Lillie Coney, Comments Before the House Committee on Science and Technology, 16 (July 1, 2010), *available at* http://epic.org/privacy/smartgrid/Smart_Grid_Testimony_2010-07-01.pdf.

88. *Id.*

89. HARRIS INTERACTIVE, PRIVACY LEADERSHIP INITIATIVE: PRIVACY NOTICES RESEARCH FINAL RESULTS, (December 2001), *available at* http://www.bbbonline.org/understandingprivacy/library/datasum.pdf.

90. *Privacy Advocates Describe Pros, Cons of Consent to Use Meter Data*, *supra* note 57.

utilities implement clear notice and consent procedures related to the smart meter data they collect and disclose.[91]

## IV. CURRENT LACK OF ADEQUATE LAWS AND REGULATIONS

Given the lack of options consumers have to address the seriousness of privacy risks inherent in smart meters, one needs to look elsewhere for privacy protection. As noted earlier, the past forty years have seen a proliferation of statutes addressing information privacy. These statutes, however, do not adequately protect electric consumers from the specific threats to privacy generated by residential smart meters.

The U.S. Congress enacted the Privacy Act of 1974 to require the use of "fair information practices," including eight principles:

> 1. There shall be no personal-data record-keeping system whose very existence is secret . . . .
>
> 2. An individual about whom information is maintained . . . shall have a right to to see and copy that information.
>
> 3. An individual about whom information is maintained . . . shall have a right to correct or amend the substance of the information.
>
> 4. There shall be limits on the types of information an organization may collect about an individual . . . .
>
> 5. There shall be limits on the internal uses of information about an individual . . . .
>
> 6. There shall be limits on the external disclosures of information about an individual . . . .
>
> 7. A record-keeping organization [must establish] reasonable and proper information management policies and practices . . . .
>
> 8. A record-keeping organization shall be accountable for its personal-data record-keeping policies, practices, and systems.[92]

These requirements would certainly help to assuage the privacy risks of smart meter data, and privacy organizations such as EPIC advocate their adoption in this regard.[93] The requirements do not have the force of law against utility companies, however, let alone third parties involved in the smart meter industry because the Privacy Protection Act of 1974 applies only to federal agencies.[94] Of the more than 3,200 traditional electric utilities in the United States, only nine are federal utilities and potentially subject to this law.[95]

---

91. NAT'L INST. OF STANDARDS AND TECH., *supra* note 11, at 105.

92. Gellman, *supra* note 18, at 3-4; *see also* 5 U.S.C. § 552a.

93. Coney, *Comments Before the House Committee*, *supra* note 85, at 12-14.

94. 5 U.S.C. § 552a(a) (2010); 5 USCS § 551(1) (2010).

95. U.S. ENERGY INFO. ADMIN., ELECTRIC POWER INDUSTRY OVERVIEW 2007, *available at* http://www.eia.doe.gov/electricity/page/prim2/toc2.html.

Two chapters within the Electronic Communications Privacy Act of 1986 (ECPA) might provide some protection against privacy risks inherent in smart meters. The Wiretap Act (18 USC §§ 2510–2522) prohibits the intentional interception and disclosure of wire, oral, or electronic communications, making such action a crime.[96] An "electronic communication" is defined by the Act as

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include:
>
> (A) any wire or oral communication [with wire communication meaning aural transmissions];
>
> (B) any communication made through a tone-only paging device;
>
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
>
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.[97]

The transmission of smart meter data either via the electric utility's wires or other broadband wire or via wireless technology falls within this definition. Therefore, hackers, war drivers, and other unauthorized users who access smart meter data as it is being transmitted either to the utility or to an in-home display—or subsequently disclose or use the data knowing it has been intercepted—violate the Act. The Wiretap Act also appears to prohibit law enforcement officials from intercepting without a warrant the smart meter data while it is in transit, unless such official is conducting "electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act."[98]

These examples of violations of the Act are not surprising, but the Act provides a few interesting exceptions to the prohibition on interception, as related to smart meter data. It states:

> It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception.[99]

The same exception is granted to a person "not acting under color of law . . . unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution of laws

96. 18 U.S.C. § 2511(1) (2010).
97. 18 U.S.C. § 2510(12) (2010).
98. 18 U.S.C. § 2511(2)(e) (2010).
99. 18 U.S.C. § 2511(2)(c) (2010).

of the United States or of any State."[100] Because the electric utility is one of the parties to the electronic communication, that is, the transmission of the smart meter data to the utility, the Wiretap Act appears to allow a utility to give permission to law enforcement or a third party to intercept the smart meter data.

The Wiretap Act further provides the following:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in an activity which is a necessary incident to the rendition of his service . . . .[101]

This provision also could permit disclosure of smart meter data by the electric utility to a third party with whom the utility has contracted to provide some aspect of the smart meter service, for example, to a home EMS, as long as the electric utility is an "electronic communication service." The ECPA defines an "electronic communication service," as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[102] An electronic communication service must be more than operation of a website.[103] Traditional electric utilities likely do not meet the definition of an electronic communication service, but an electric utility that provides users the ability to send smart meter data to the utility and then instructions back to smart appliances arguably fits the definition. This would mean, however, that the electric utility is both the provider of the service and a recipient of communications using the service. The applicability of this definition to an electric utility providing smart meter service has not yet been tested in the courts. If there is a match, then the Wiretap Act permits the electric utility to share smart meter data with third parties who are *necessary* to the provision of the smart meter service, although it is unclear who will decide which third parties are *necessary*. These exceptions suggest that, without further clarification by the courts, the Wiretap Act will not adequately protect the information privacy of consumers with smart meters in their homes.

Another chapter of the ECPA (18 USC §§ 2701–2709), known as the Stored Communications Act (SCA), might be an alternative guarantor of

100. 18 U.S.C. § 2511(2)(d) (2010).
101. 18 U.S.C. § 2511(2)(a)(i) (2010).
102. 18 U.S.C. § 2510(15) (2010).
103. *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 307 (E.D. N.Y. 2005).

privacy protection for smart meter data. The Act addresses the unlawful access to stored communications. Its prohibitions include:

> 1. a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
>
> 2. a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—
>
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing or communications received by means of electronic transmission from), a subscriber or customer of such service; . . . and
>
> 3. a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.[104]

Whether or not these prohibitions apply to an electric utility depends on whether an electric utility can be classified as an entity providing "electronic communication service to the public."[105]

As discussed above, an electric utility providing smart meter service arguably is an electronic communication service, although this premise has not been tested in the courts. The SCA further requires, however, that this service be provided "to the public." One court found that, while the statute does not define "public," the term is unambiguous and means the "aggregate of citizens" or "the community at large."[106] If the electric utility is providing smart meter service, including the communication of data to and from the utility, to the community where it offers electric service and if that community must get its electric service from that utility, the electric utility then provides "electronic communication service to the public." That service is an integral part of the utility's business.

Assuming for the moment that the SCA's general prohibitions apply to electric utilities providing smart meter service, one must still determine whether any of the SCA's exceptions to the prohibitions apply. Under the statute, a provider of an electronic communication service to the public may disclose the contents of a communication:

---

104. 18 U.S.C. § 2702(a) (2010).

105. Whether or not these prohibitions apply to a third party provider of smart meter data analysis (e.g., a home energy management service) will depend on whether the third party can be classified as a remote computing service. However, before addressing that issue, which is more tenuous, one needs to address whether the electric utility can disclose smart meter data to the third party, and this article will focus on the latter.

106. Anderson Consulting LLP v. UOP, 991 F. Supp. 1041, 1042 (N.D. Ill. 1998).

> (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient; . . . [or]
>
> (3) with the lawful consent of the originator or an addressee or intended recipient of such communication; . . . [or]
>
> (5) as may be necessary incident to the rendition of the service or to the protection of the rights or property of the provider of that service.[107]

The electric utility is arguably the intended recipient of the smart meter data when it is sent from the consumer's home to the utility. As long as there is no interdiction against being both the provider of the service and an intended recipient of a communication,[108] then the utility may disclose the contents of smart meter data to one of its agents, for example, a third party vendor of a home EMS or related smart meter devices, either because that third party provider is an agent or because the utility, as intended recipient, lawfully consents to the disclosure. Even if the utility were found not to be an intended recipient, it could still disclose the data to a third party if doing so were necessary to providing the full smart meter service, including data analysis, to its electric customers. The utility could disclose the smart meter data to a law enforcement or governmental agency, however, only if the utility "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure" or the utility is presented with a valid warrant, with limited exceptions.[109]

If the conditional conclusions stated above are true, then the SCA offers very little privacy protection relative to smart meter data. Given the newness of smart meters, however, uncertainties exist regarding the electric utility's classification as an electronic service provider, the application of the term "public" to the population required to participate in smart meter electric service, and the possibility of being simultaneously an electronic service provider and an intended recipient of smart meter data. These uncertainties make it impossible to determine whether the SCA offers any protection from the disclosure of intimate personal data from smart meters.

Two other federal statutes that could offer a modicum of information privacy protection for smart meter customers include the Computer Fraud and Abuse Act (CFAA) and Section 5 of the Federal Trade Commission Act (FTC Act). The CFAA provides for criminal penalties in the case of intentional unauthorized access (or access that exceeds authorization) of certain computers, including "protected" computers.[110] A "protected computer" may be one "which is used in interstate or foreign commerce or

107. 18 U.S.C. § 2702(b) (2010).
108. As noted above, this conclusion has not been tested in the courts.
109. 18 U.S.C.S. § 2702(b)(8) (2010); 18 U.S.C.S. § 2703(LEXIS 2010).
110. 18 U.S.C.S. § 1030(a)(2) (2010).

communication."[111] Because smart meters are part of a smart grid with transmission wires crossing state lines (with the exceptions of Texas, Hawaii and Alaska[112]), interstate commerce is affected, so smart meters and the utility servers that contain smart meter data would be protected computers. The CFAA therefore clearly prohibits the criminal conduct of hackers, war drivers, and rogue utility employees who intentionally exceed authorized access certainly threaten the privacy of consumers' smart meter data. The more insidious threats to information privacy posed by smart meters—seemingly authorized conduct by utilities, law enforcement officials, and third parties—are not addressed by the CFAA.

Section 5 of the FTC could help to address some of the latter threats. That statute states that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[113] The FTC has litigated cases to enforce the promises companies make in their privacy statements, "including promises about the security of consumers' personal information."[114] For this law to provide any real protection for electric consumers' personal information, utilities and authorized third parties with access to smart meter data must have privacy policies continually in place that truly do allow consumers to have well-informed, proactive control over that data. No current federal statutes *consistently* require such privacy policies or the policies contain serious exceptions, and, as noted *supra*, consumers rarely read privacy statements—especially the fine print. Public utility commission regulations may limit disclosures by utilities of personal information, but such regulations also do not necessarily require utilities to have company privacy policies.[115]

When it comes to smart meter data, state laws and state regulatory requirements—like federal statutes—do not provide adequate information privacy protection. The results of NIST's privacy impact assessment reveal that, "in general, state utility commissions currently lack formal privacy policies or standards related to the Smart Grid."[116] Current public utility

111. 18 U.S.C.S. § 1030(e)(2) (2010).

112. The Texas Interconnected System is not interconnected with the Eastern or Western Interconnected Systems, other two major interconnected power grids in the United States, (except by certain direct current lines). U.S. Energy Info. Admin., *supra* note 95. However, almost all U.S. utilities are interconnected with at least one other utility by the Eastern or Western Interconnected Systems except for in Alaska and Hawaii. *Id.*

113. 15 U.S.C. § 45(a)(1) (2010).

114. *Enforcing Privacy Promises: Section 5 of the FTC Act*, Fed. Trade Comm'n, http://www.ftc.gov/privacy/privacyinitiatives/promises.html.

115. *See, e.g.*, Rule 4 CCR 723-1:1104.

116. NAT'L INST. OF STANDARDS AND TECH., *supra* note 11, at 103.

commission regulations, while possibly forbidding utilities from disclosing a customer's personal information without customer permission, do not define "personal information." For a traditional utility, a customer's personal information would be limited to customer name, address, possibly social security number, and billing information. Smart meter data, as detailed earlier in this article, reveal much more personal information. Current commission regulations may also allow exceptions to disclosure. The COPUC rules, for example, while prohibiting disclosure of personal information to a third party without customer authorization, permit a utility to

> disclose personal information requested by a federal, state, or local governmental agency including, but not limited to: the Commission; state and local departments of social services; and federal, state, and local law enforcement agencies. Written requests shall be on official letterhead. In the case of a telephone request, the employee of the regulated entity shall verify the caller's identity by obtaining the caller's office telephone number and returning the call, unless the employee knows the caller is an authorized governmental representative. A person requesting information in person shall demonstrate that he or she properly represents a governmental agency.[117]

The rules do not limit the information that a governmental agency may receive and do not require a warrant or court order. While the COPUC is currently reviewing its regulations regarding smart meter data, law enforcement and other governmental agencies may currently obtain smart meter data on 10,000 households where Xcel Energy has installed smart meters and appliance control devices, using the data as they deem appropriate.

In Illinois, where 131,000 customers have smart meters, the Public Utilities Act has similar disclosure provisions. The Act allows for general customer usage to be disclosed, but forbids disclosure of "customer specific billing, usage or load shape data" to alternative retail electric suppliers and local units of government without customer authorization.[118] However, it permits disclosure to a customer's "agent" and appears to be silent on disclosure to other third parties.[119] The Act does provide that a "public utility shall not disclose customer record information to a law enforcement agency unless the law enforcement agency requests the customer record information in writing, specifying that the information is necessary for a law enforcement purpose."[120] As in Colorado, the utility need not receive a warrant or court order to release the personal information.

---

117. Rule 4 CCR 723-1:1104, *supra* note 115, at (d).
118. 220 ILL. COMP. STAT. 5/16-122 (2010).
119. *Id.*
120. 220 ILL. COMP. STAT. 5/5-110 (2010).

As more utilities install smart meters, more states and public utility commissions will likely start reviewing and updating their laws and regulations to address smart meter issues, like the privacy of smart meter data. The results are unpredictable. In any case, the states' efforts might be irrelevant given the interstate nature of the smart grid with transmission wires crossing state lines. Furthermore, many individual utilities provide electric service in more than one state and sometimes consolidate their billing operations in just one of the states they serve or even outsource their billing to another state. Because interstate commerce is impacted, federal statutes may pre-empt state laws and regulations.

## V. THE FOURTH AMENDMENT

If existing statutes and regulations do not protect the privacy of smart meter data that reveals activities occurring inside the home, perhaps the Fourth Amendment offers some protection, at least against law enforcement's unfettered access to the data. 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 persons or things to be seized.[121]

The U.S. Supreme Court has upheld this right to be free from unreasonable search and seizure, but the definition of "unreasonable" remains fluid. In *United States v. Katz*, the Court held that what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[122] A concurring opinion in that case set out a twofold requirement for reasonableness: (1) "[A] person [must] have exhibited an actual (subjective) expectation of privacy" and (2) "the expectation [must] be one that society is prepared to recognize as 'reasonable.'"[123] A case decided four years later explicitly stated that the Fourth Amendment "is ruled by fluid concepts of 'reasonableness.'"[124] In 1979, the Court decided that the subjective expectation that phone numbers—once dialed— will remain private was not an expectation "that society is prepared to recognize as reasonable."[125] Seven years later, Congress enacted the Pen Register Act as part of the ECPA to protect the privacy of outgoing phone numbers. As technology evolved further, law enforcement agencies gained the capability

121. U.S. CONST. amend. IV.
122. 389 U.S. 347, 351-52 (1967).
123. *Id.* at 361 (Harlan, J., concurring).
124. United States v. White, 401 U.S. 745, 753 (1971).
125. Smith v. Maryland, 442 U.S. 735, 743 (1979) (quoting Katz, 389 U.S. at 361).

of detecting activity within a home by using thermal imaging. In 2001, the Court held that warrantless use of the technology to view inside a home was prohibited by the Fourth Amendment.[126] Warning that use of thermal imaging could disclose intimate details about personal activities, including "at what hour each night the lady of the house takes her daily sauna and bath," Justice Scalia opined that the Fourth Amendment "draws 'a firm line at the entrance to the house.' That line, we think, must be not only firm but also bright."[127] These cases generally suggest that the Fourth Amendment would prohibit access by law enforcement to smart meter details that might reveal intimate details about activities occurring within a customer's home.

The courts' interpretations of Fourth Amendment law, however, raise two caveats. First, while Justice Scalia insisted in *United States v. Kyllo* that a firm, bright line be drawn at the entrance to the house, he also stated there that "'intrusion into a constitutionally protected area,' constitutes a search—at least where . . . the technology in question is not in general public use."[128] 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. As smart meters become more prevalent, with more than fifty million installed by 2012, along with home EMSs that connect the smart meters to smart appliances and other smart devices, it is foreseeable that society could find it unreasonable to expect that one's electricity-consuming activities inside the home would remain private.

Second, the Court "consistently has held that a person has no legitimate expectation of privacy in information that he voluntarily turns over to third parties."[129] This information may include "numerical information" given to companies "in the ordinary course of business."[130] Courts reason that, because there is no privacy interest in records kept in the course of a business, individuals cannot challenge law enforcement's acquisition of various types of information such as bank records, credit card statements, and cell phone records.[131] Using the same reasoning, courts have held that individuals do not possess a reasonable expectation of privacy in utility records—at least in the kilowatt consumption data contained in electric

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

127. *Id.* at 38-40 (citation omitted).

128. *Id.* at 34. (citation omitted).

129. Smith, 442 U.S. at 743-44.

130. United States v. Suarez-Blanca, 2008 U.S. Dist. LEXIS 111622, 25 (N.D. Ga. 2008).

131. *See, e.g.*, United States v. Miller, 425 U.S. 435, 442-43 (1976); United States v. Phibbs, 999 F.2d 1053, 1077-78 (6th Cir. 1993); United States v. Hynson, 2007 U.S. Dist. LEXIS 67261, 15 (E.D. Pa. 2007)

utility records.[132] The court in one such case, however, qualified its reasoning by pointing out that the records contained only the amount of power consumed and did not reveal "any intimate details of [defendant's] life."[133] Given the rich detail of smart meter data, which can reveal intimate details about the electric customer's life, and the reality that electric customers have no true choice in whether or not to give the data to the utilities, courts might find this data beyond the warrantless reach of law enforcement. On the other hand, the data is part of the utility's business record, and as smart meters become commonplace, courts could find that individuals cannot realistically have an expectation of privacy in the data generated by the meters—or, at least, an expectation that society will find reasonable.

## VI. CURRENT THREATS AND LOOMING UNCERTAINTY BEG IMMEDIATE ACTION

Given the unprecedented threats smart meters pose to the privacy of activities that occur inside the home and the lack of protection provided by current laws and regulations against these threats, new avenues of protection must be enacted now—before, as Quinn warned, "one really salient privacy invasion . . . makes the front page of the *New York Times* and the *Washington Post*" and brings smart grid development to an unplanned halt.[134] When faced with the same challenge in Ontario, Canada, where every house in the province will have a smart meter by the end of 2010, the province's information and privacy commissioner "put[] up a big stop sign" until the province could implement a "privacy-by-design" approach to smart meter data.[135] She explained that "[r]egulatory compliance often comes in after the data breaches have happened . . . . I wanted the protections to be proactive and preventative."[136] It is unwise to wait until someone uses personal smart meter data to imitate pleaserobme.com, a website that aggregated and streamed information from various social networking services that encouraged users to share their locations throughout the day, revealing when their homes were unoccupied.[137]

---

132. *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, 2010 U.S. Dist. LEXIS 44960, 17-18 (E.D. Va. 2010).

133. State v. Kluss, 867 P.2d 247, 254 (Idaho Ct. App. 1993).

134. *Smart Grid Elevated to Top Issue by Leading Privacy Watchdogs*, *supra* note 8.

135. *Ontario's Privacy Commissioner Urges Halting Smart Grid*, SMARTGRIDTODAY, (April 8, 2010), http://www.smartgridtoday.com/public/1447.cfm?sd=31.

136. *Id.*

137. *Please Rob Me: Site Tells the World When You're Not Home*, HUFFINGTON POST, (April 19, 2010), http://www.huffingtonpost.com/2010/02/17/please-rob-me-site-tells_n_465966.html.

Privacy advocates, governmental agencies, and those involved in the booming smart meter industry generally agree on the need for some type of action and have proposed various approaches. One approach is to rely on the electric utilities to protect their customers' privacy. After all, they have a great deal at stake in the success of smart meters. In comments on NIST's first draft of the *Smart Grid Cyber Security Strategy and Requirements* interagency report, PEPCO, an electric company serving the District of Columbia and parts of Maryland, suggested that "[t]he current process for tariff approval adequately considers customer privacy."[138] Even NIST appears to support a modified version of this approach, noting the each organization should have its own disclosure requirements (subject to applicable laws and regulations) and its own retention guidelines for smart meter data.[139] In addition, utilities must comply with their own published privacy statements per the requirements of Section 5 of the FTC Act.

There are, however, several reasons reliance on utilities will not ensure privacy protection of customers' personal information from smart meters. As virtual monopolies within their service areas, electric utilities have limited incentives to appease consumers. While they might have much at stake in the success of smart meters, the utilities' operating costs and investments are reimbursed by ratepayers, greatly minimizing the utilities' risk. The nature of utilities is also changing given the enormous amount of personal information they are beginning to collect from customers.[140] As Polonetsky points out, "Utilities understand the regulated environment and basic security. But they have not been involved with issues such as profiling, tracking and third-party data transfers because those have not been part of their business models."[141] Compared to online companies, for example, they have much less experience dealing with privacy issues.[142]

Another approach is to develop and then rely on standards and recommended privacy practices—the focus of NIST.[143] The president of the IEEE Standards Association asserts that "[a]t the end of the day, it's all about standards. If we get that right at the onset, we create an ecosystem for

138. NAT'L INST. OF STANDARDS AND TECH., *supra* note 10, at 159.

139. *Id.* at 7, 205.

140. Ann Cavoukian, *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid*, INFORMATION AND PRIVACY COMMISIONER, ONTARIO, CANADA (June 2010) (on file with author), http://www.ipc.on.ca/images/Resources/achieve-goldstnd.pdf.

141. *Privacy Advocate Details Weaknesses in Smart Grid*, *supra* note 40.

142. Susan Lyon, *Privacy Lessons SmartGrid Should Take from Web 2.0*, ELECTRIC LIGHT & POWER (April 1, 2010), http://www.elp.com/index/display/article-display/9627238375/articles/utility-automation-engineering-td/volume-15/Issue-4/Features/Privacy-Lessons-SmartGrid-Should-take-from-WEB-20.html.

143. NAT'L INST. OF STANDARDS AND TECH., *supra* note 11, at 6-7, 10, 104–09.

the development of technologies that will thrive in the present and future."[144] NIST's work is well researched. Its impressive working group conducted a privacy impact assessment and considered more than 450 comments from privacy groups, utilities, technology firms, and other entities involved in the smart grid industry when compiling its second draft of *Smart Grid Cyber Security Strategy and Requirements* interagency report (and is now working on a third version).[145] The problem with relying on a standards and privacy guidelines approach, however, is that the NIST report contains only recommendations despite the term "requirements" in the report's title. NIST clearly states this in the report itself, noting that the report contains "suggested privacy practices," "regulations are outside the scope" of the project, "enforcement is outside the scope," and the second draft of the report "has been revised to clarify that the information is guidance, not mandatory."[146] While NIST and others hope that state regulators and the industry will embrace the guidelines, everyone is free to ignore them or simply pick and choose the recommendations they like.

If relying solely on the utilities to ensure customer privacy is too risky and the NIST guidelines are only that—guidelines—then perhaps a third approach would work: look to the state public utility commissions to use the NIST guidelines and regulate how electric utilities implement privacy protections. One clear advantage to this approach is its ability to require utility compliance because public utility commissions have regulatory authority over utilities. As NIST observes, most commissions also have customer privacy policies in place—albeit ones that pre-date smart meters—and utilities take commission policies very seriously.[147] In some states where smart meter rollout started early, commissions have begun to update their regulations and, as part of that process, are examining the issue of customer privacy. For example, in August 2009, the COPUC opened a docket in the matter and officially requested comments from interested parties in February 2010.[148] In response to state legislation, the Public Utilities Commission of the State of California also began a process in late 2008 to institute rulemaking to "Actively Guide Policy in California's De-

144. Chuck Adams, *Smart Grid Standards: Why Are They Needed and How Will They Work?*, CONNECTED PLANET (April 7, 2010), http://connectedplanetonline.com/commentary/smart-grid-standards-0407/.

145. NAT'L INST. OF STANDARDS AND TECH., *supra* note 11, at 5–6, App. G; Press Release, NIST Released the Second Draft, *supra* note 16.

146. NAT'L INST. OF STANDARDS AND TECH., *supra* note 10,at 196, 199, 235.

147. NAT'L INST. OF STANDARDS AND TECH., *supra* note 11, at 103 n. 28.

148. Order Seeking Comments and Information: In the Matter of the Investigation of Security and Privacy Concerns regarding the Deployment of Smart-Grid Technology, Decision No. C10-0175, (February 24, 2010), *available at* https://www.dora.state.co.us/pls/efi/EFI_Search_UI.Show_Decision?p_session_id=&p_dec=13823.

velopment of a Smart Grid System" and issued a decision in June 2010.[149] Public utility commissions in other states have received federal funding to study the smart grid.[150] As these studies progress, commissions will likely generate smart-meter related rules governing electric utility conduct, which the U.S. Supreme Court has termed "one of the most important of the functions traditionally associated with the police power of the States."[151]

Some argue, however, that delegating the protection of customers' privacy to state public utility commissions may not be adequate to ensure their privacy given the unprecedented threats posed by smart meter data. Inconsistencies could arise between state laws and commission regulations because other state agencies often have responsibility for the enforcement of state privacy laws.[152] New commission regulations might not be sufficient given the pressure commissions feel to support the smart meters from federal and state governments, utility lobbyists, and third parties poised to benefit from the installation of smart meters and related devices. For the third parties, there is big money at stake, and these companies' business models rely on obtaining smart meter data.[153] In Colorado, for example, the COPUC recognized the potential for trade-offs "between protecting privacy and promoting innovation" and asked those commenting on proposed rules for the deployment of smart meters to address the trade-offs.[154] In October 2009, California's governor signed into law SB 17, mandating that the state's public utility commission work with utilities to ensure that smart meter deployment plans are ready for rollout in a fairly short timeframe.[155] The commission specifically required the utilities to discuss in their deployment plans how they will "[e]nable maximum access by third parties to the grid, creating a welcoming platform for deployment of a wide range of energy technologies and management services."[156] The commission also acknowledged that it might need to review and approve individual utility

149. Decision Adopting Requirements for Smart Grid Deployment Plans Pursuant to Senate Bill 17 (Padilla), Chapter 327, Statutes Of 2009, Decision 10-06-047 (June 24, 2010), *available at* http://docs.cpuc.ca.gov/PUBLISHED/FINAL_DECISION/119902.htm [hereinafter *Decision 10-06-047*].

150. Press Release, Illinois Commerce Commission, ICC Receives Federal Grant to Study Smart Grid, Energy Reliability (June 21, 2010) (on file with author), *available at* http://www.icc.illinois.gov/press/.

151. Ark. Elec. Coop. Corp. v. Ark. Pub. Serv. Comm'n, 461 U.S. 375, 377 (1983).

152. NAT'L INST. OF STANDARDS AND TECH., *supra* note 11,at 103; *see also Decision 10-06-047*, *supra* note 149, at 43 n.90.

153. Alicia Caldwell, *The Grid*, DENVER POST, Dec. 13, 2009, *available at* http://www.denverpost.com/opinion/ci_13972530.

154. Decision No. C09-0878, App. A (August 12, 2009), *available at* http://www.dora.state.co.us/puc/DocketsDecisions/HighprofileDockets/09I-593EG.htm.

155. *Decision 10-06-047*, *supra* note 149, at 6.

156. *Id.* at 34.

plans before the commission can "address customer access and specific privacy and cyber security rules in a separate phrase."[157] Further, the commission recognized that it may lack authority over third parties.[158] Even if all of these challenges could be overcome, the interstate nature of the smart grid—and probable travel of smart meter data across state lines—might negate the ability of state public utility commissions and legislatures to address the privacy threats posed by smart meter data.

Another source for privacy protection could be federal legislation. Historically, Congress has addressed gaps in laws generated by new technology. For example, after the U.S. Supreme Court held that it was not reasonable to expect phone numbers once dialed to be private, Congress passed the Pen Register Act,[159] although confusion still exists regarding reasonable privacy expectations for cordless phones.[160] Congress also has enacted legislation when issues implicate interstate commerce, such as the Telecommunications Act of 1996, which requires telecommunications carriers to obtain customer authorization before disclosing "customer proprietary network information" (CPNI).[161] The Act defines CPNI as

> (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
>
> (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.[162]

Smart-meter data bears strong similarities to CPNI, suggesting that federal legislation as related to electric utilities would be appropriate. Furthermore, federal agencies have already entered the fray regarding use of the smart grid, such as NIST's work on interoperability standards, the Federal Energy Regulatory Commission (FERC) rulemaking that is to follow the conclusion of NIST's work, and the Federal Communication Commission (FCC) National Broadband Plan.[163]

---

157. *Id.* at 42, 121.

158. *Id.* at 42-43.

159. Pen Register – Further Readings, http://law.jrank.org/pages/9137/Pen-Register.html (last visited July 30, 2010)

160. Frierson v. Goetz, 99 Fed. Appx. 649, 654 (6th Cir. 2004).

161. 47 U.S.C. § 222(c)(1) (2010).

162. 47 U.S.C. § 222(h)(1) (2010).

163. FED. ENERGY REGULATORY COMM'N, SMART GRID STANDARDS ADOPTION: STAFF UPDATE AND RECOMMENDATIONS (July 15, 2010), *available at* http://www.ferc.gov/legal/staff-reports/07-15-10-smart-grid.pdf; BROADBAND.GOV, NATIONAL BROADBAND PLAN: 12.1 BROADBAND AND THE SMART GRID, *available at* http://www.broadband.gov/plan/12-energy-and-the-environment/#s12-1 (last visited Oct. 15, 2010).

While the National Association of Regulatory Utility Commissioners urges Congress and federal agencies to "respect and incorporate State rules and ongoing State authority to protect ratepayers' privacy" and wants to limit federal agency involvement to setting voluntary standards, neither seems likely to occur.[164] Several pieces of legislation are now pending related to the smart grid. The proposed Cybersecurity Act of 2009 mandates NIST to recommend standards for cyber security and allocates funds to the National Science Foundation for research on how to guarantee individual privacy in cyberspace.[165] It also requires the President to review existing federal privacy laws, such as the ECPA, and report to Congress.[166] None of these provisions actually provides specific protection of smart meter data; in fact, the proposed act gives the Secretary of Commerce "access to all relevant data concerning such networks without regard to any provision of law, regulation, rule, or policy restricting such access."[167] Two companion bills in Congress, S. 3487 and H. R. 5696, both known as the "e-KNOW Act," give each consumer who has a smart meter the right to access the data generated by the smart meter in that consumer's home, with the House bill also limiting the utility's ability to disclose the data to third parties and prohibiting any third party's disclosure of the data without the consumer's informed, written consent.[168] The future of these Congressional bills is uncertain, but they might set a floor for privacy protection related to smart meter data upon which state legislation, like California's SB 837, can build.

As the national rollout of smart meters continues state by state with the addition to HANs of smart appliances, home EMS, and other smart devices, the data collected and shared will pose unprecedented threats to the privacy most Americans expect to enjoy in their homes. Yet Americans cannot simply refuse smart meters and disconnect themselves from the electric grid. Current laws and regulations do not adequately protect their privacy; in fact, a series of U.S. court cases suggests that electric consumers do not possess a reasonable expectation of privacy in utility records. While standards currently being developed, updates to individual electric company privacy policies, and yet-to-be-determined state regulations might offer a modicum of protection, new federal legislation specifically address-

164. NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS, COMMITTEE RESOLUTIONS 17 (July 21, 2010), *available at* http://summer.narucmeetings.org/2010SummerFinalResolutions.pdf.

165. S. 773, 111th Cong. §§ 6(a), 11(a)(4) (2009).

166. *Id.* § 16.

167. *Id.* § 14(b)(1).

168. S. 3487, 111th Cong. (2010); H. R. 5696, 11th Cong. (2010); *available at* http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.5696:.

ing smart meter data might be the only route to ensure that Americans truly have in the future a right to privacy in their homes.