UCLA LAW REVIEW

Smart Meters, Smarter Regulation: Balancing Privacy and Innovation in the Electric Grid

Samuel J. Harvey

ABSTRACT

Transitioning from our current energy infrastructure to a smart grid will be essential to meeting future challenges. One key component of the smart grid is advanced metering infrastructure (AMI). AMI allows for the grid to be run more effectively and efficiently by making granular near real-time data about customers' energy usage available. Coupled with the input and innovation of third-party companies and researchers, the potential benefits of this technology are immense.

But given the granularity of AMI data, some academics and consumer advocates are concerned that the technology could place customer privacy at risk. It is therefore essential that regulators appropriately tailor privacy protections to strike the proper balance between the innovative potential of AMI data and consumers' privacy concerns. When possible, regulators should opt for regimes allowing for the protected sharing of granular AMI data with third parties.

AUTHOR

Sam Harvey is a student at the University of California, Los Angeles School of Law. He is interested in how creative legislative and regulatory approaches can channel public and private innovation into meaningful solutions to pressing national and global issues.

He would like to sincerely thank Professor Ann Carlson for her support, feedback, and inspiration. He is grateful to the *UCLA Law Review* staff for their exceptional work in editing this piece.

TABLE OF CONTENTS

INTRODUCTION

America's energy infrastructure is crumbling. Crucial upgrades will be needed if our nation is going to meet the demands of the next century and successfully transition to a clean energy future. One proposed solution is to develop a smart grid by automating and computerizing the existing generation, transmission, and distribution infrastructure.[1] A key technology associated with the smart grid is advanced metering infrastructure (AMI). This set of technologies allows for detailed, near real-time data[2] about consumer energy usage to be generated and transmitted to electricity service providers.[3] The range of potential benefits of AMI is immense. Unfortunately, the detailed and near real-time nature of the AMI data may create privacy concerns for some customers. This Comment addresses the privacy concerns associated with AMI adoption and recommends policy considerations that can guide regulators in addressing these concerns while ensuring that the full range of benefits can be realized.

Part I introduces the smart grid and AMI. These technologies consist of an array of sensors and transmitters that enable two-way digital communication between grid operators and sites throughout the grid. The benefits that could be realized from these technologies are immense and will be felt by consumers, utilities, businesses, and society as a whole. Furthermore, the level of innovation that third-party researchers and businesses can offer will be essential to realizing the full potential of these technologies.

Part II explains the highly detailed level of electricity usage information AMI can make available and the potential privacy concerns this raises. AMI generates an unprecedented level of data about a customer's electricity usage. Analyzing the energy usage patterns of a single home can be essential to many of AMI's benefits. But this data can potentially be used to paint a detailed

1. EXEC. OFFICE OF THE PRESIDENT, A POLICY FRAMEWORK FOR THE 21ST CENTURY GRID: ENABLING OUR SECURE ENERGY FUTURE 3 (2011), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf; *What is the Smart Grid?*, U.S. DEPT. OF ENERGY, https://www.smartgrid.gov/the_smart_grid (follow "The Smart Grid" hyperlink).

2. Current smart meters typically measure electricity usage at fifteen-minute intervals. *Smart Meter Texas, Frequently Asked Questions*, PUB. UTIL. COMM'N OF TX., *available at* http://www.puc.texas.gov/industry/projects/electric/34610/AMITMtg052411/SMT_FAQ.doc; *Smart Meters: Frequently Asked Questions*, LONG ISLAND POWER AUTH., http://www.lipower.org/SMART/faq.html.

3. ELECTRIC POWER RESEARCH INST., ADVANCED METERING INFRASTRUCTURE (AMI) 1 (2007), *available at* http://www.ferc.gov/eventcalendar/Files/20070423091846-EPRI%20-%20Advanced%20Metering.pdf.

picture of energy users' daily habits. As the technology improves, this can lead to concerns that customer privacy will not be adequately protected. This Part discusses the ways in which these concerns vary depending on whether AMI data is sought by utilities, third-party researchers and companies, or law enforcement.

Part III discusses key considerations for forming regulatory frameworks that adequately address AMI data privacy concerns. Customer adoption of new technologies is essential to their success. Therefore, AMI deployment on a significant scale will require regulations that address customers' privacy concerns. Classification of different types of data based on the accompanying privacy risk will also be essential for developing appropriately tailored regulations. Customer-specific data containing personally identifiable information (PII), for example, deserves the most protection, while aggregated data that does not contain PII and reflects energy usage at a neighborhood or regional level requires less protection. Information that is specific to individual customers but has been stripped of PII likely falls in a middle zone. The aim of this Comment is to propose an approach that strikes the proper balance between achieving the goals of AMI and effectively addressing privacy concerns.

I. THE SMART GRID AND AMI

Our nation's power infrastructure—the grid—is being strained to its limits. From outages due to extreme weather to the threat of cyberattacks to the need to revolutionize our energy consumption to combat climate change, the grid's ability to adequately meet these challenges is seriously in doubt. Of the five massive blackouts over the last four decades, three have occurred in the last nine years.[4] Additionally, some of the grid's generation, transmission, and distribution facilities date back as far as the 1880s.[5] The American Society of Civil Engineers recently gave America's energy infrastructure a D+ grade, citing the grid's advanced age as a key concern.[6] In the age of smartphones and instant worldwide interconnectivity, there is a profound irony in relying on a

4. U.S. DEP'T OF ENERGY, THE SMART GRID: AN INTRODUCTION 7 (2008), *available at* http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf ("Today, the irony is profound: In a society where technology reigns supreme, America is relying on a centrally planned and controlled infrastructure created largely before the age of microprocessors that limits our flexibility and puts us at risk on several critical fronts . . . .").

5. AM. SOC'Y OF CIVIL ENG'RS, 2013 REPORT CARD FOR AMERICA'S INFRASTRUCTURE 1 (2013), *available at* http://www.infrastructurereportcard.org/a/documents/Energy.pdf (last visited May 17, 2014).

6. *Id.*

grid that was designed when Thomas Edison's light bulb was still a novelty.[7] The result is that our grid, "the largest interconnected machine on Earth,"[8] is barely meeting our needs. It is clear that a major system-wide overhaul will be needed if we are to address the myriad challenges facing our energy infrastructure.

One of the most popular proposals calls for transitioning to a smart grid.[9] Generally, the smart grid involves computerizing and automating the existing system by introducing two-way digital communication between grid operators and sites throughout the grid. This is achieved through the introduction of sensors and transmitters that generate near real-time energy usage data and allow for remote operation of grid components.[10] Other industries already use many of the technologies required to modernize our energy infrastructure, but the energy sector has been slow to adapt these technologies.[11]

Chief among the technological upgrades essential to the smart grid is advanced metering infrastructure (AMI). AMI technologies enable electricity service providers to track consumer energy usage in near real-time.[12] Smart meters are an essential component of AMI. Unlike traditional electricity meters, which simply measure total electricity usage, smart meters track a home's usage measured in near real-time.[13] The result is a detailed picture of a customer's load profile—a customer's electricity usage described as it changes over time. This data allows customers to assess their consumption at a more detailed level and, armed with that information, better alter their behavior to reduce energy bills. Smart meter data also enables utilities to more effectively operate the grid.

According to the U.S. Department of Energy, "A truly smart grid should achieve environmental goals at lower cost than the traditional grid, be able to respond more quickly to natural or man-made outages and, overall, operate the electrical system more efficiently without reducing system cyber

7. *See supra* note 4.
8. *Id.* at 5.
9. *See generally,* EXEC. OFFICE OF THE PRESIDENT, *supra* note 1.
10. *Smart Grid*, U.S. DEP'T OF ENERGY, http://energy.gov/oe/technology-development/smart-grid (last visited Oct. 15, 2013).
11. *Id.*
12. *See* ELECTRIC POWER RESEARCH INST., *supra* note 3; People *ex rel.* Madigan v. Illinois Commerce Comm'n, 967 N.E.2d 863, 867 (Ill. App. Ct. 2012) ("One of the building blocks of the new technology is AMI, which consists of a communication system, advanced meters, and computer software and hardware to process the information collected from the new meters.").
13. SmartMeter™ meters used by PG&E record residential customer usage hourly and commercial usage in fifteen-minute intervals. *What is a SmartMeter™?,* PAC. GAS & ELEC. CO., http://www.pge.com/en/myhome/customerservice/smartmeter/index.page (last visited Oct. 1, 2013).

security or reliability."[14] In short, upgrading to a smart grid will create benefits for consumers, utilities, businesses, and society as a whole.

The real-time nature of AMI data will enable consumers to make smarter, more efficient, and more cost-effective energy consumption choices. Instead of waiting for an electricity bill at the end of the month, consumers will be able to see their current usage and shift consumption from more expensive peak usage periods to cheaper, lower demand periods. Additionally, consumers will be able to identify sources of excessive energy usage in their homes, such as inefficient appliances, and make appropriate upgrades. Syncing a home's power consumption with the Internet will also enable users to turn appliances on and off remotely. This feature is not only convenient, but will also allow consumers to lower their electricity bills even further by raising awareness of current usage and allowing people to switch off forgotten and unneeded appliances while outside the home.[15]

The smart grid will also enable utilities to provide better service at a reduced cost.[16] For instance, utilities often learn of a power outage only after a customer calls to report it.[17] Through the smart grid, a utility company would immediately find out an outage had occurred, identify the cause, and pinpoint which customers had been affected. A smart grid's early notification and enhanced diagnostics would enable utilities to quickly reroute electricity to customers, thereby reducing the impact of an outage.[18] Additionally, utilities would be able to address problems before service disruptions occur. As one regulatory researcher explains, "utilities will be able to monitor the health of the grid proactively, allowing them to repair pending faults in advance and avoid outages."[19] Enhanced monitoring of the location and timing of electricity needs will also mean utilities will be able to better reduce line loss—

14. SHERRY LICHTENBERG, NAT'L REGULATORY RESEARCH INST., SMART GRID DATA: MUST THERE BE CONFLICT BETWEEN ENERGY MANAGEMENT AND CONSUMER PRIVACY? 1 (2010), *available at* http://webapp.psc.state.md.us/Intranet/CaseNum/NewIndex3_VOpenFile.cfm?filepath=%5C%5CColdfusion%5CEWorkingGroups%5CDRDG%5C%5CSmart%20Grid%20Implementation%5CNRRI_smart_grid_privacy_dec10-17.pdf (quoting Addressing Policy and Logistical Challenges to Smart Grid Implementation, 75 Fed. Reg. 57,006, 57,007 (request for information Sept. 17, 2010)).
15. *Id.* at 9.
16. *Id.* at 11.
17. *See, e.g.*, GEN. ELEC., RELIABILITY MESSAGING SHEET 2 (2009), http://www.ge-energy.com/content/multimedia/_files/downloads/Reliabilty_Messaging_Sheet-04_09_09.pdf.
18. *Id.*; *see, e.g.*, EXEC. OFFICE OF THE PRESIDENT, ECONOMIC BENEFITS OF INCREASING ELECTRIC GRID RESILIENCE TO WEATHER OUTAGES 10 (2013), *available at* http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.
19. LICHTENBERG, *supra* note 14, at 14.

energy lost in transmission or distribution—and avoid the need for excess generation to ensure demand is met.[20]

There could also be a vast array of benefits to business because the smart grid can spur the growth of entirely new companies and products. For example, companies like Google and Cisco are developing products to enable customers to better analyze the real-time data that smart meters generate and better manage their consumption.[21] Appliance manufacturers are also developing smart appliances that will interface with the new grid and allow customers greater freedom to monitor and adjust their consumption.[22] Additionally, companies offering energy efficiency audits will be able to use AMI to better analyze customers' usage habits and recommend efficiency upgrades.[23]

Probably the greatest beneficiary of the smart grid will be society as a whole, which could experience economic, environmental, and even national security benefits.[24] The economy will benefit from fewer and shorter outages thanks to more effective grid operation and experience lower energy costs thanks to consumer behavioral changes and more efficient and accurate pricing.[25] It is estimated that building the smart grid will create 280,000 new jobs, half of which will remain after completion for ongoing operation and upkeep.[26] Additionally, consumer access to usage data will result in lower overall power consumption, saving money on energy bills and simultaneously providing global benefits.[27] In testimony submitted by Google to the California Public Utilities Commission (CPUC), the company explained that customers who

20. TOM SIMCHAK & LOWELL UNGAR, REALIZING THE ENERGY EFFICIENCY POTENTIAL OF SMART GRID 4 (2011), *available at* http://www.ase.org/sites/ase.org/files/ASE-smart_grid_white_paper_0.pdf ("Smart grid capabilities across the transmission and distribution (T&D) network can allow T&D systems to operate more efficiently and responsively, reducing line losses and reducing excess generation needed to ensure grid stability. Smart grid systems would allow improved awareness of T&D system conditions in real time. This would allow the grid to be operated with tighter margins of error—and thus more efficiently.").

21. *See, e.g.*, LICHTENBERG, *supra* note 14, at 12.

22. *See id.*

23. *See, e.g.*, *SolarCity Energy Explorer Energy Efficiency Program*, SOLARCITY, http://www.solarcity.com/energy-efficiency/#/~/average-yearly-total (last visited Dec. 18, 2013).

24. U.S. DEP'T OF ENERGY, NAT'L ENERGY TECH. LAB., UNDERSTANDING THE BENEFITS OF THE SMART GRID 2 (2010), *available at* https://www.smartgrid.gov/sites/default/files/doc/files/Understanding_Benefits_Smart_Grid_201003.pdf.

25. *Id.* at 9 ("Broader Societal Benefits [of the smart grid]: Downward pressure on prices—through improved operating and market efficiencies, reduced supply cost resulting from peak reductions, consumer involvement, and deferral of future capital projects. Overall, markets will be more efficient, resulting in the economically correct prices for electricity, which are expected to be less than they would have been without the capabilities of the smart grid.").

26. *Id.*

27. LICHTENBERG, *supra* note 14, at 14.

can see their energy use in real time save at least 5 to 15 percent, and "[i]f just half of American households cut their demand by 10 percent . . . the CO_2 emissions avoided would be equal to taking approximately 8 million cars off the road."[28] Reduced consumption would mean lower emissions from power plants and a reduced need to construct new generating capacity. The smart grid would also enable smoother integration of new technologies, such as electric car powering stations and renewable energy in the form of distributed generation.[29] The result would be lower dependence on conventional fossil fuels and overseas oil, providing both environmental and national security benefits. As one report explained, "U.S. dependence on oil weakens international leverage, undermines foreign policy objectives, and entangles America with unstable or hostile regimes."[30] Greater reliance on domestic renewable energy sources could reduce the weight energy needs are given in foreign policy decisions, thereby benefiting U.S. national security.

These myriad smart grid benefits will not be attainable simply through the actions of governments and utilities. The active involvement of third parties, such as research institutions and private companies that focus on energy efficiency, demand response, and distributed generation, will be essential.[31] Just

28. Comments of Google on Smart Grid Technology Deployment in California, Rulemaking 08-12-009, at 5 (Cal. Pub. Util. Comm'n Feb. 9, 2009), http://docs.cpuc.ca.gov/PublishedDocs/EFILE/CM/97193.PDF.

29. U.S. DEP'T OF ENERGY, WHAT THE SMART GRID MEANS TO YOU AND THE PEOPLE YOU REPRESENT 3 (2009), *available at* http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Regulators.pdf. Distributed generation refers to decentralized, small-scale electricity production facilities located at or near sites of consumption and can include a variety of renewable energy technologies such as solar photovoltaic systems, wind turbines and fuel cells. CAL. PUB. UTIL. COMM'N, BIENNIAL REPORT ON IMPACTS OF DISTRIBUTED GENERATION 2-1, 2-2 (2013), *available at* http://www.cpuc.ca.gov/NR/rdonlyres/29DCF6CC-45BC-4875-9C7D-F8FD93B94213/0/CPUCDGImpactReportFinal2013_05_23.pdf; *Distributed Energy*, U.S DEP'T OF ENERGY, http://energy.gov/oe/technology-development/smart-grid/distributed-energy.

30. CNA CORPORATION, POWERING AMERICA'S DEFENSE, at vii (2009), *available at* http://www.cna.org/sites/default/files/Powering%20Americas%20Defense.pdf.

31. *See, e.g.*, NRDC Comments on Assigned Commissioner's Scoping Memo and Ruling Amending Scope of Proceeding to Seek Comments and to Schedule Workshops on Energy Data Center, Rulemaking 08-12-009, at 1, 3 (Cal. Pub. Util. Comm'n Dec. 17, 2012), http://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M039/K595/39595938.PDF ("Better analysis is critical to the growth of the efficiency services sector, to facilitate delivery of efficiency programs, and to promote innovation and market transformation by enabling companies to provide new products and service using the customer information. . . . [I]n many cases, utilities are not in a good position to deliver the needed analysis and should not be burdened with engaging in exploratory inquiries or socializing the findings. It is important to establish the ability for research institutions to have some defined access to [AMI] data to perform research."); Joel B. Eisen, *Who Regulates the Smart Grid?: FERC's Authority Over Demand Response Compensation in Wholesale Electricity Markets*, 4 SAN DIEGO J. CLIMATE & ENERGY L. 69, 70–71(2013) ("A relatively new set of players has recently begun to participate in wholesale energy markets,

as the Internet spurred an information technology revolution by providing a platform for private and corporate innovation, the smart grid can facilitate the creation of a new generation of companies and products geared towards lowering consumer energy bills and meeting the challenges faced by our energy infrastructure.[32] These companies and inventions will, in turn, increase the grid's ability to provide the vast array of envisioned benefits.[33] As a result, it is crucial to adopt policies that facilitate third-party access to AMI data so that the full range of benefits can be realized. Unfortunately, while the positive transformative potential of AMI and the smart grid is immense, these technologies are not without potential drawbacks.

II. PRIVACY CONCERNS

Privacy is one of the greatest concerns for modern customers. Traditional electricity meters measure only a customer's cumulative energy usage, which is usually read monthly.[34] Smart meters, on the other hand, measure energy usage far more frequently, such as every fifteen minutes.[35] The current

offering a different commodity: 'demand response' (DR). . . . These new firms will aggregate consumer agreements to refrain from using electricity, and offer the block of resulting reductions in demand for sale in the wholesale energy markets. . . . It is an interactive and dynamic application that can spur the growth of other two-way uses of a Smart Grid, such as greater incorporation of distributed energy resources. For this reason, DR is the Smart Grid's 'killer app.'").

32. John Podesta, *How Smart Grids Fit Into the Clean Energy Challenge: Remarks as Delivered at the 2nd Annual GridWise Global Forum*, AM. PROGRESS (Nov. 10, 2011), *available at* http://www.americanprogress.org/issues/green/news/2011/11/14/10558/how-smart-grids-fit-into-the-clean-energy-challenge. *See also* Jeff St. John, *An "Energy Data Center" for California's Smart Grid?*, GREENTECH MEDIA (Nov. 15, 2012), http://www.greentechmedia.com/articles/ read/an-energy-data-center-for-californias-smart-grid ("[T]he [California Public Utilities Commission] has been trying to make smart grid data as open and accessible as possible . . . to as wide a set of third-party software, hardware and service providers as possible, to jumpstart a market for smart grid-to-home energy efficiency.").

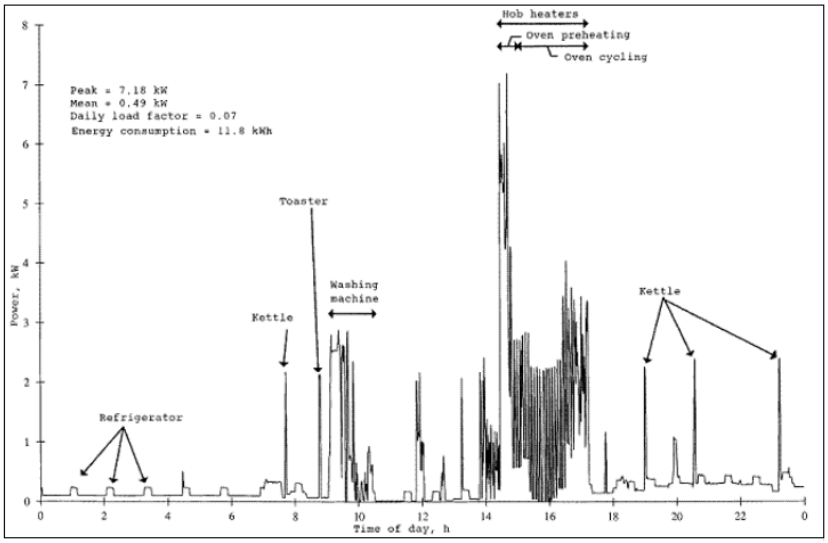
33. EXEC. OFFICE OF THE PRESIDENT, VICE PRESIDENT OF THE UNITED STATES, THE RECOVERY ACT: TRANSFORMING THE AMERICAN ECONOMY THROUGH INNOVATION 40 (2010), *available at* http://www.whitehouse.gov/sites/default/files/microsites/Recovery_Act.PDF ("The two-way flow of information from the grid to customers creates new opportunities in the private sector for innovation in the development of tools for consumers. The development of these tools will enable both the utilities and consumers to use electricity more efficiently, thereby reducing their costs.").

34. BRANDON J. MURRILL ET AL., CONG. RESEARCH SERV., R42338, SMART METER DATA: PRIVACY AND CYBERSECURITY 3 (2012), *available at* http://www.fas.org/sgp/crs/misc/ R42338.pdf.

35. Data is generated on a real-time or near real-time basis. This is usually at least hourly, but often every fifteen or even five minutes. CHERYL DANCEY BALOUGH, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161, 166 (2011).

technology could likely even be used to measure usage in one-minute intervals.[36] As Figure 1 below illustrates, matching usage data from future minute-to-minute meter readings with the known load signatures of certain appliances would reveal when an appliance is being used in a home.[37] While this graph overstates the ability of currently deployed technologies, it is illustrative of what experts expect to be readily available from subsequent generations of AMI.[38]

FIGURE 1: Identification of Appliances from Real-Time Electricity Usage Data[39]



This information could reveal a great deal about occupants' behavior and habits in the home. For instance, a home's load profile could reveal occupants' daily schedules by tracking when the kettle or hot water heater turns on, when

36. MURRILL, *supra* note 34, at 4.
37. *Id.* ("By examining smart meter data, it is possible to identify which appliances a consumer is using and at what times of the day, because each type of appliance generates a unique electric load 'signature.'").
38. U.S. DEP'T OF ENERGY, DATA ACCESS AND PRIVACY ISSUES RELATED TO SMART GRID TECHNOLOGIES 9 (2010), *available at* http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf ("The current state of the art, in terms of the granularity of data collected by utilities using advanced metering, cannot yet identify individual appliances and devices in the home in detail, but this will certainly be within the capabilities of subsequent generations of Smart Grid technologies.") [hereinafter DOE, DATA ACCESS AND PRIVACY].
39. M. NEWBOROUGH & P. AUGOOD, DEMAND-SIDE MANAGEMENT OPPORTUNITIES FOR THE UK DOMESTIC SECTOR 287 (1999), *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=790574.

the garage door opens and closes, or when an electric vehicle is plugged in.[40] This data can also reveal whether a home security system has been activated, if someone uses certain medical equipment, or when the television is on.[41] One study even found that analyses of household usage could reveal which television channel or video content occupants were viewing.[42]

It is clear that plentiful AMI data could be analyzed to reveal a highly detailed picture of someone's private life. As a result, it is unsurprising that utility customers may be concerned about how this data is handled. In order to develop new regulatory regimes to meet this privacy challenge, it is helpful to look at the rules and legal structures currently governing access to similar data by utilities, researchers and private companies, and law enforcement.

A. Utilities

Utility companies have long amassed significant amounts of data in the form of cumulative monthly electricity usage and personal billing information. This information has traditionally included names, addresses, bank account information, and even social security numbers.[43] As a result, utilities and their regulators usually have policies in place that forbid the disclosure of these types of personal information.[44] According to the U.S. Department of Energy, utilities and regulators have a strong track record of protecting private customer data.[45] The concern, however, is that utilities and regulators have yet to develop privacy policies that adequately account for the new types of data AMI will make available.[46] Fortunately, a number of state public utility commis-

40. MURRILL, *supra* note 34, at 4–5.
41. BALOUGH, *supra* 35, at 167.
42. ULRICH GREVELER ET AL., MULTIMEDIA CONTENT IDENTIFICATION THROUGH SMART METER POWER USAGE PROFILES 1, *available at* http://epic.org/privacy/smartgrid/smart_meter.pdf ("Our research shows that the analysis of the household's electricity usage profile . . . does reveal what channel the TV set in the household was displaying. It is also possible to identify . . . audiovisual content in the power profile that is displayed on a CRT, a Plasma display TV or a LCD television set with dynamic backlighting. Our test results indicate that a 5 minutes-chunk of consecutive viewing without major interference by other appliances is sufficient to identify the content."); Elinor Mills, *Researchers Find Smart Meters Could Reveal Favorite TV Shows*, CNET (Jan. 24, 2012, 11:15 AM), http://news.cnet.com/8301-27080_3-57364883-245/researchers-find-smart-meters-could-reveal-favorite-tv-shows.
43. BALOUGH, *supra* 35, at 182.
44. *Id.* at 181–82.
45. DOE, DATA ACCESS AND PRIVACY, *supra* note 38, at 3.
46. BALOUGH, *supra* 35, at 181 ("[I]n general, state utility commissions currently lack formal privacy policies or standards related to the Smart Grid." (quoting NAT'L INST. OF STANDARDS AND TECH., SMART GRID CYBER SECURITY STRATEGY AND REQUIREMENTS, DRAFT 2 at 103 (Feb. 2010))).

sions are considering and adopting new privacy regulations that address AMI data.[47] Additionally, some utilities have pointed out that smart meters eliminate the need for in-person meter readers who must enter a customer's property to read and record usage, thereby actually reducing some privacy intrusion.[48] Whether customers' AMI privacy concerns will outweigh the benefit of no longer having a monthly visitor on their private property remains to be seen. Nonetheless, it is clear that utilities have a strong record of customer privacy protection that they will want to maintain as AMI systems come online. Thus, AMI data may not present a completely novel challenge for the industry, but the new range of analysis available for AMI data underscores the importance of continuing to ensure utility customers' privacy protections.

B. Third-Party Researchers and Companies

Privacy concerns become more acute when third parties seek access to AMI data. Third-party researchers and companies are seeking access to this data in order to identify customers, enhance product design, and conduct more in-depth analysis of energy consumption.[49] For example, a company could use AMI data to identify potential customers that could benefit from energy efficiency upgrades. That company could then market products and services tailored specifically for those individual customers.[50] Third-party companies are already developing data management software to enable utilities to better compile and analyze the vast amounts of data now made available to them by AMI.[51] General Electric has developed an entire wireless network system aimed at allowing utilities to monitor and operate a smart grid.[52] The smart

47. *See, e.g.*, SAN DIEGO GAS & ELEC. CO., ANNUAL STATUS REPORT OF SAN DIEGO GAS & ELECTRIC COMPANY (U 902 E) FOR SMART GRID DEPLOYMENTS AND INVESTMENTS, Rulemaking 08-12-009, at 36 attach. A (2008), *available at* http://www.cpuc.ca.gov/NR/rdonlyres/455178B7-ADF5-44E6-B11A-614CED98AFD6/0/SDGE_Annualy_Report_ Smart_Grid_Deployment.pd.

48. *Smart Meter*, GA. POWER, http://www.georgiapower.com/residential/products-programs/smart-meter (last visited Mar. 20, 2014).

49. AUDREY LEE ET AL., ENERGY DATA CENTER BRIEFING PAPER 1 (2012), *available at* http://www.cpuc.ca.gov/NR/rdonlyres/8B005D2C-9698-4F16-BB2B-D07E707DA676/0/ EnergyDataCenterFinal.pdf.

50. *Id.*

51. *See, e.g.*, Jeff St. John, *Oracle's Many Paths to Smart Grid Analytics*, GREENTECH MEDIA (Sep. 26, 2013), http://www.greentechmedia.com/articles/read/Oracles-Many-Paths-to-Smart-Grid-Analytics; Jeff St. John, *Siemens, eMeter Push Smart Meter Data and Analytics to the Cloud*, GREENTECH MEDIA (Oct. 24, 2013), http://www.greentechmedia.com/articles/read/siemens-emeter-push-smart-meter-data-and-analytics-to-the-cloud.

52. *Grid IQ™ AMI P2MP*, GEN. ELECTRIC, https://www.gedigitalenergy.com/smartmetering/catalog/p2mp.htm#p2mp4.

grid would greatly benefit from allowing third-party developers access to AMI data in order to help craft solutions and advancements for utilities and consumers. Allowing greater third-party access would create "new opportunities in the market for the development of energy saving products,"[53] and in that way further the goals of the smart grid.[54]

While utilities and the state regulatory agencies that govern them generally have strong track records of protecting the privacy of customer information,[55] the multitude of third parties who could seek access to AMI data presents a novel and understandably daunting privacy challenge. Heavily regulated utilities holding private data is one thing, but granting access to unvetted third-party researchers and companies could compromise personal customer information.

An important part of effectively and safely sharing AMI data is anonymization, which involves presenting data in such a way that it cannot be linked to individual users. Two common methods of anonymization are aggregation and deidentification. These two concepts can be employed either individually or jointly and are at the center of policy debates over the safe sharing of AMI data.

First, aggregation involves processing data in clusters to dilute individual-level records.[56] The resulting aggregated data reflects "consumption on a neighborhood or other regional level."[57] As a result, the data would show total or average usage for a group of customers without identifying those customers or attributing specific usage data to an individual.[58] Although not every aggregation regime is guaranteed to thwart manipulation to identify specific households,[59] the practice does provide significant protection. But it could also reduce the usefulness of the data to third parties. For instance, a company wishing to de-

53. LEE ET AL., *supra* note 49, at 4.
54. Third parties can play a pivotal role in enabling consumers to access their data, thereby saving money on electricity bills and reducing consumption. Such access ensures that the benefits of the smart grid are realized. DOE, DATA ACCESS AND PRIVACY, *supra* note 38, at 3.
55. *Id.* ("DOE commends the utilities' strong track record of protecting the privacy of customer data and acknowledges the traditional responsibility of state utility commissions in regulating issues associated with data privacy.").
56. Working Group Report Pursuant to February 27, 2013 Administrative Law Judge's Ruling, Rulemaking 08-12-009, at 5 app. A (Cal. Pub. Util. Comm'n July, 10 2013), http://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M076/K995/76995999.PDF [hereinafter Working Group Report].
57. DOE, DATA ACCESS AND PRIVACY, *supra* note 38, at 30.
58. Working Group Report, *supra* note 56, at 38 ("[A]ggregated data would not include the total annual or average annual energy usage for an individual household, precisely because the data pertains to a specific household.") (internal quotations omitted).
59. *Id.* ("Despite excluding micro-data, aggregated data can still leak private information.").

velop an energy efficiency plan to market to specific households or a researcher looking at individual customer behavior in the smart grid may find aggregated data too broad.

The second method of protecting data is deidentification. This method involves removing personally identifying information, such as name, address, account number, and other billing information, from electricity records.[60] Unlike aggregation, deidentification could make data available at the single-home level, although third parties would not be able to assign that profile to an actual customer or location. The result would be data that was not linkable to an individual but was still customer specific, and could therefore be analyzed at a granular and detailed level.

But anonymization, whether through aggregation, deidentification, or some combination of the two, is not without its drawbacks. An emerging body of research points to a growing consensus among scientists that "anonymizing data to sufficiently prevent re-identification of an individual is almost impossible."[61] This is because anonymized data can be compared to information in external databases. A detailed load profile of a home can be used to identify specific individuals by comparing it to outside information, such as public traffic schedules, mobile phone location records, travel schedules, social media, and even firsthand observation.[62] As one computer security and privacy expert explained, "mounting a de-anonymization attack against an anonymized load profile is computationally cheap, and the side information required only needs to be vaguely related to occupancy—and as such is plentiful and in the hands of many third parties."[63] As a result, even with anonymization measures in place, it is often possible to reverse engineer the data in order to identify individuals.[64] In one instance, a Massachusetts state agency released state employee health records stripped of all explicit identifiers. A

60. *See* ERIKA MCCALLISTER ET AL., NAT'L INST. OF STANDARDS & TECH., SPEC. PUB. 800-122, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII): RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ES-3 (2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf ("Organizations can de-identify records by removing enough PII such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. De-identified records can be used when full records are not necessary, such as for examinations of correlations and trends.").

61. Administrative Law Judge's Ruling Adding Technical Memos to the Record, Rulemaking 08-12-009, at 5 attach. B (Cal. Pub. Util. Comm'n May 13, 2013), *available at* http://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M064/K670/64670678.PDF.

62. *See id.* attach B. app. A, at 21.

63. *Id.* at 22.

64. *See id.*

computer science researcher was able to reidentify individual employees from the supposedly anonymized data. She was even able to reidentify the governor's health records and, "in a theatrical flourish," mailed them to his office.[65]

In light of these acknowledged shortcomings, experts are increasingly seeking solutions that "balance the risks and value of data sharing in a de-identification regime."[66] The result is that a privacy protection regime will need to see anonymization techniques as only a partial solution to privacy concerns.

C. Law Enforcement

Utility customers and privacy advocates may also have concerns about law enforcement access to the vast amount of detailed AMI data. Even before the advent of smart meters, law enforcement agencies sought electricity usage data in order to investigate crimes, such as indoor marijuana cultivation.[67] Granular AMI data presents a potential new tool for law enforcement to investigate a much broader set of crimes or even track people's whereabouts.

The Fourth Amendment provides that, "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[68] Yet the U.S. Supreme Court has consistently found that individuals have no reasonable expectation of privacy in information they willingly convey to third parties.[69] This third-party doctrine has been held to include information provided to businesses by customers[70] and utility records have traditionally fallen under this rule.[71] As a result, law enforcement is not required to obtain a warrant to access that information.[72]

Nonetheless, the Supreme Court has repeatedly affirmed the importance of the home as the location afforded the most privacy under the

65. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1720 (2010).

66. Email from Salil Vadhan, Vicky Joseph Professor of Computer Sci. and Applied Mathematics, Harvard Univ., to Department of Health and Human Serv., Office of the Sec'y (Oct. 26, 2011), *available at* http://privacytools.seas.harvard.edu/files/privacytools/files/commonruleanprm.pdf.

67. *See, e.g.*, Jordan Smith, *APD Pot-Hunters are Data-Mining at AE*, AUSTIN CHRON., (Nov. 16, 2007), http://www.austinchronicle.com/news/2007-11-16/561535 (reporting on Texas law enforcement's use of utility records to find customers with atypical energy usage that may point to marijuana cultivation).

68. U.S. CONST. amend. IV.

69. *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

70. See *id.*

71. *See* MURRILL ET AL., *supra* note 34, at 15.

72. *See, e.g.*, *Smith*, 442 U.S. at 745–46 (holding that, because petitioner revealed the phone numbers he dialed to the telephone company, the installation and use of a "pen register" to record the numbers petitioner dialed "was not a 'search,' and no warrant was required").

Fourth Amendment.[73] The sanctity of the home in Fourth Amendment jurisprudence, coupled with the level of detailed information about the interior of a home available in AMI data, may prompt a shift away from the third-party doctrine.[74] Such a development would provide needed protection to utility customers as AMI deployment continues.

Before the use of smart meters, the CPUC set policies in place to address the issue of law enforcement access to customer utility information. In 1990, the commission issued an order prohibiting utilities from releasing customer-specific information to law enforcement agencies without a subpoena or warrant.[75] This approach has been echoed in a set of model smart grid data privacy policies generated by the Vermont Law School Institute for Energy and the Environment.[76] By extending protection beyond that provided by the Fourth Amendment, these regulations better address the privacy concerns presented by AMI data while maintaining clear procedures for law enforcement to follow in order to gain access to customer information. Both the CPUC policies and the Vermont Law School model regulations therefore provide a helpful blueprint for regulators to follow as they grapple with balancing consumer privacy concerns against the needs of law enforcement.

The advent of AMI and other smart grid technologies holds tremendous potential for meeting our modern energy challenges. But the amount of private information that these technologies collect creates legitimate privacy concerns. These concerns are particularly acute when AMI data is shared with third parties. Given the importance of third-party researchers and companies in achieving the aims of the smart grid, new privacy regimes will need

73. For example, in *Silverman v. United States*, Justice Stewart, writing for the majority, stated "At the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." Silverman v. United States, 365 U.S. 505, 511 (1961). In *Kyllo v. United States*, the court held unconstitutional the warrantless use of a thermal imaging device to detect heat from lamps in a marijuana cultivation operation. Key in this decision was the observation that monitoring heat signatures potentially reveals a wide array of intimate details about the inside of a home that could not otherwise be acquired without physical intrusion. Kyllo v. United States, 533 U.S. 27, 37–40 (2001).

74. *See* MURRILL ET AL., *supra* note 34, at 16–17.

75. Re Competitive Access to Customer List Information, Decision 90-12-121, 39 CPUC 2d 173 (Cal. Pub. Util. Comm'n Dec. 27, 1990), *as constructed in* Re Competitive Access to Customer List Information, Decision 91-10-036, 41 CPUC 2d 483 (Cal. Pub. Util. Comm'n Oct. 23, 1991).

76. Colin Hagan & Katie Thomas, *A Model Privacy Policy for Smart Grid Data* 11 (Nov. 4, 2011) (unpublished working paper) (on file with Institute for Energy and the Environment at Vermont Law School), *available at* http://www.vermontlaw.edu/Documents/Smart%20grid%20privacy%20policy%2043FB8CE1d01.pdf ("Privacy includes a customer's right to keep confidential knowledge of any activities undertaken inside his or her home and evident from the customer's electricity us[e] [*sic*] data, except to the extent that a warrant compels disclosure to state or federal law enforcement officials.").

to strike an appropriate balance between spurring innovation through access to data and ensuring customer privacy is vigorously protected.[77]

III. BALANCING PRIVACY NEEDS AND SMART GRID GOALS

The task of regulating AMI data to ensure privacy while furthering important policy goals is daunting. Regulatory agencies' policies will need to be reviewed and revised as technologies change and new concerns arise.[78] This Part lays out general considerations policymakers should take into account and discusses specific rules and regulations that could be implemented to reflect these considerations.

In some instances, AMI and smart meters have sparked controversy,[79] and public backlash has even led some municipalities to oppose or ban their deployment.[80] While privacy has not been the only issue at stake in these incidents, it has certainly been one of the most prominent.

The ultimate success or failure of AMI will depend on customer acceptance.[81] While it may be easy for experts to point out that many of the controversies are unfounded or sensationalist,[82] addressing public concerns

77. *See* LICHTENBERG, *supra* note 14, at 19–20.

78. *See id.* at 35 ("As consumers, utilities, and regulators learn more about the smart grid, regulators should review, evaluate, and modify regulations to cover new issues and remove regulations that are no longer useful.").

79. *See, e.g.*, BOB GOHN & CLINT WHEELCOCK, PIKE RESEARCH, SMART GRID: TEN TRENDS TO WATCH IN 2011 AND BEYOND 5 (2010), *available at* http://www.navigantresearch.com/wordpress/wp-content/uploads/2010/10/SG10T-10-Pike-Research.pdf (describing the "Bakersfield Effect," which refers to "loud consumer pushback" on smart meters, in California from 2009 to 2010 because of privacy and potential health concerns).

80. *See, e.g.*, *id.* (citing Maryland as an example of a state that initially rejected a smart meter plan in response to the "ruckus" and only later approved it "with significant strings attached"); INST. FOR ENERGY & THE ENV'T, VT. LAW SCH., CVPS SMARTPOWER: A SMART GRID COLLABORATION IN VERMONT 23 (2012), http://www.vermontlaw.edu/Documents/IEE/CVPS-SmartGrid-Report-Final-120215.pdf [hereinafter IEE REPORT] (noting that "those expressing such concerns [about smart grid projects] in Vermont have become more vocal"); Chris Hooks, *As Towns Say No, Signs of Rising Resistance to Smart Meters*, N.Y. TIMES (May 18, 2013), http://www.nytimes.com/2013/05/26/us/as-texas-towns-say-no-signs-of-rising-resistance-to-smart-meters.html?_r=1& (noting that two Texas towns, Brady and Camp Wood, have "placed a moratorium on smart meter installation").

81. *See* BETH KARLIN, *Public Acceptance of Smart Meters: Integrating Psychology and Practice*, *in* ACEEE SUMMER STUDY ON ENERGY EFFICIENCY IN BUILDINGS: FUELING OUR FUTURE WITH EFFICIENCY 1 (2012), http://www.aceee.org/files/proceedings/2012/data/papers/0193-000243.pdf ("Public acceptance of utility programs and initiatives is vital for efficient deployment. Consumer complaints, protests, and lawsuits, can significantly impede progress and cost utilities, cities, and taxpayers money. . . . While the advantages of smart meters are widely accepted by utilities, academics, and governments, some communities have experienced backlash and disapproval from customers.").

82. *Id.*

will be critical to successful implementation of the smart grid. Therefore, creating an open dialogue to educate customers and hear privacy concerns will be critical for any regulatory regime.[83]

Given the necessity of addressing privacy concerns while deploying AMI technologies, it will be crucial for any regulatory structure to tailor protection measures to the level of risk posed by different types of data while maximizing the benefits that disclosure to third parties can offer. There are numerous ways to separate data into categories, but broadly speaking, data can be organized in the following three types: (1) customer-specific data containing personally identifying information; (2) customer-specific data stripped of personal identifiers but still indicating usage for single homes; and (3) aggregated data representing neighborhood- or community-level information.[84] As third parties increasingly seek access to AMI data, policymakers will need to consider the characteristics of these types of data and cater regulatory regimes to both maximize AMI benefits and minimize privacy risks.

A. Customer-Specific Data Containing Personally Identifying Information (PII)

Consumer-specific data containing PII generates the greatest privacy concern and should therefore be afforded the greatest level of regulatory protection. Utilities have long held customer-specific PII, such as names, addresses, and bank account information for the purpose of billing customers.[85] But different privacy protections will likely be needed if this type of data is to be shared with third parties. CPUC privacy rules limit the allowable uses of "covered information," which it defines as "usage information obtained through . . . [AMI] when associated with any information that can reasonably be used to identify an individual, family, household, residence, or non-residential customer . . . ."[86] This definition certainly covers usage data that contains PII. Under these California privacy rules, customer data with PII may be used

83. IEE REPORT, *supra* note 80, at 19–20 ("Recognizing the important role that customers' actions will play in the success of the smart grid, CVPS has committed to provide early and ongoing education. . . . This education and outreach campaign included surveys, focus groups, and a well-developed print, radio, television, and social media campaign.").

84. *See generally* Working Group Report, *supra* note 56, at 15, 18.

85. *See* BALOUGH, *supra* note 35, at 181–82.

86. Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company, Rulemaking 08-12-009, at 1 attach. C & D (Cal. Pub. Util. Comm'n proposed May 6, 2011), *available at* http://docs.cpuc.ca.gov/PublishedDocs/PUBLISHED/GRAPHICS/140370.PDF.

without customer consent only for programs necessary to grid operation that the CPUC, utilities, or third parties under contract with utilities carry out.[87] All other uses, including third-party commercial access, require customer consent.[88] Other states follow similar rules regarding disclosure of PII to third parties. For instance, Vermont's utility smart grid partnership, eEnergy Vermont, requires consent for disclosure of customer-specific billing information.[89]

Like under CPUC privacy rules, exceptions should be made for third parties contracting with utilities or regulators to perform services essential to meeting system-wide goals and requirements. For example, one Michigan utility company advocating for a plan similar to that used in California cited "sharing [PII] to enable energy efficiency contractors to help achieve statutorily mandated annual energy savings goals" as an instance where customer consent should not be required.[90] These disclosures could take place under the oversight of the utility or regulatory body with strict non-disclosure and privacy measures in place to minimize risks.[91] Therefore, any AMI data protection regime should require customer consent for the transmission of PII to third parties, except in those instances where third parties are operating under the supervision of utilities to carry out essential grid operating functions.

One benefit of this regulation is that it tracks customer expectations that private utility data will only be used for the effective provision of electrical services. Furthermore, the privacy risks associated with PII substantially outweigh the benefits of broad disclosure. If PII were made widely available, companies could customize products and marketing for specific customers and contact them directly. This might mean customers who would not ordinarily consent to have their information transmitted to a third party would adopt energy-saving products once the potential cost reductions were illustrated to them. While this could result in wider adoption of new technologies and greater reductions in energy consumption, these benefits would likely not outweigh the accompanying privacy concerns. Furthermore, requiring customer consent for the disclosure of identifying data seems to be a fairly well-

87. *See, e.g.*, *id.* at 2, 7.
88. *See, e.g.*, *id.* at 2, 10.
89. *See* IEE REPORT, *supra* note 80, at 23.
90. Consumers Energy Company's Comments, Case No. U-17102, at 3 (Mich. Pub. Serv. Comm'n Dec. 17, 2012) (discussing Consumers Energy Company's assertion that consent should not always be required for disclosure of PII to third parties).
91. *See id.*

established norm.[92] Consumers would likely be uneasy knowing their PII was being made widely available to third parties without their express consent.

In the case of customer-specific data containing PII, there is a fairly clear consensus that customer consent should be required for all third-party access other than that necessary for the effective running of the grid by utilities and regulators.[93] This would prevent third-party companies from obtaining PII without consent for private marketing purposes but allow utilities and regulators to take advantage of the resources and expertise of third parties to better run and regulate a smart grid electrical system.

B. Customer-Specific Deidentified Data

The second category of data is customer-specific usage data that has been stripped of PII. This category is subject to greater disagreement over how to strike the proper balance between access and privacy. The key issue with this type of data is the risk that it could be manipulated to reidentify individual households.

Some academics and consumer advocates argue that the risk of reidentifying individuals by reverse engineering deidentified data means this type of data should be treated the same as data with PII.[94] These parties have pointed out that it is often difficult to tell if data has been sufficiently deidentified because the ability to reidentify data is dependent on the various external databases available to match against the AMI data.[95] Additionally, the technological

92. *See, e.g.*, U.S. DEP'T OF EDUC., THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT: GUIDANCE FOR ELIGIBLE STUDENTS 3 (2011), http://www2.ed.gov/policy/gen/guid/fpco/ferpa/students.html ("[A] school may not generally disclose personally identifiable information from an eligible student's education records to a third party unless the eligible student has provided written consent."); CAL. OFFICE OF PRIVACY PROT., RECOMMENDED PRACTICES ON CALIFORNIA INFORMATION-SHARING DISCLOSURES AND PRIVACY POLICY STATEMENTS 13 (2008), *available at* http://oag.ca.gov/sites/all/files/pdfs/privacy/COPP_bus_reportinfo_sharing1.pdf; *Standards for Privacy of Individually Identifiable Health Information*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm (last updated July 6, 2001) ("[This rule] establishes a federal requirement that most doctors, hospitals, or other health care providers obtain a patient's written consent before using or disclosing the patient's personal health information to carry out treatment, payment, or health care operations . . . .").

93. Hagan & Thomas, *supra* note 76, at 4 (stating that utilities may disclose data, including PII, to third-party contractors when "necessary to provide reliable electric service[,]" including for billing and software purposes, but that third-parties will be contractually obligated to maintain confidentiality).

94. *See, e.g.*, Working Group Report, *supra* note 56, at 34–44.

95. *See* Opening Comments of the Electronic Frontier Foundation on Energy Data Center, Rulemaking 08-12-009, at 9 (Cal. Pub. Util. Comm'n Dec. 17, 2012), *available at* http://docs.cpuc.ca. gov/PublishedDocs/Efile/G000/M042/K160/42160299.PDF.

ability to manipulate data is constantly changing, so data that is sufficiently deidentified today might become readily reidentifiable tomorrow.[96] But given that deidentified data does not, on its face, identify individual customers or households, this data does not need to be subject to the same restrictions as customer-specific data containing PII in order to strike the proper balance between privacy and innovation.

One potential tool for minimizing privacy risks while maximizing the availability of useful granular data is the energy data center (EDC). EDCs are repositories for energy data from utility companies that enable access by third parties, the public, and policymakers. For example, the State of New Jersey EDC employs a user-friendly website through which researchers, businesses, and the general public can access aggregated energy data.[97] In California, one proposal envisions using an EDC to facilitate the safe sharing of deidentified data.[98] Under such plans, the EDC would act as an intermediary between the utility company and third parties, allowing companies that offer solar installation and energy efficiency services to access "anonymized, household level energy consumption and billing data."[99] The EDC would be a centralized database under the strict regulation of the CPUC, perhaps operated by another state government agency such as the University of California.[100] The EDC would strip household level data of PII before transmitting it to third parties. Businesses would then analyze this data, develop proposals catered to specific households and transmit this information back to the EDC. Customers could then opt-in to allow the EDC to send them these proposals.[101] This use of the EDC attempts to maximize the innovative potential of AMI data while protecting consumers' PII.

As discussed in Part II, however, there is a growing consensus that "anonymizing data to sufficiently prevent reidentification of an individual is almost impossible."[102] While some may argue this means household level deidentified data should never be transmitted to third parties without customer consent, protections can likely be put in place to allow sufficient shar-

96. *See id.* at 34.
97. *See* STATE OF NEW JERSEY ENERGY DATA CENTER, http://www.njenergydatacenter.org (last visited Mar. 20, 2014).
98. *See* Working Group Report, *supra* note 56, at 70.
99. *Id.*
100. St. John, *supra* note 32.
101. *See* Working Group Report, *supra* note 56, at 70.
102. Admin. Law J.'s Ruling Adding Technical Memos to the Record, Rulemaking 08-12-009, at 5 attach. B (Cal. Pub. Util. Comm'n May 13, 2013), *available at* http://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M064/K670/64670678.PDF.

ing of data to promote the benefits of AMI while limiting the risk of deidentification and other privacy breaches.

For instance, the Federal Trade Commission (FTC) has recommended a series of protections that companies can take to minimize deidentification risks. First, the data transferor (the EDC in the above example) would need to be confident that the data could not "reasonably be used to infer information about, or otherwise be linked to, a particular customer."[103] This would be a flexible standard that would take into consideration the type of data transmitted and its envisioned use, such as whether it would be published externally.[104] Second, a company acquiring such data, like a solar installer or energy efficiency services provider, would be required to publicly attest to refraining from attempts to reidentify individuals represented by the deidentified data.[105] Third, the transferor would contractually require the recipient to refrain from attempting to reidentify individuals based on the data.[106]

Developing a disclosure regime around these protocols would allow regulations to be effective in the face of evolving reidentification techniques. Given that the ability to reidentify data is constantly changing, any rule that distinguished merely between what is reidentifiable and what is not would soon be outdated. The FTC recommendations work by simply requiring third parties to pledge and certify that they will not attempt to reidentify data regardless of whether reidentification is possible. Provided these rules could be effectively implemented and enforced, they could enable lasting regulation of PII-stripped household level data. In this way, they would provide a sustainable means of balancing the promise of AMI data with privacy concerns.

C. Aggregated Data

The final category is aggregated data, which is less granular than the prior two forms because it represents usage at the community or regional rather than individual level. Aggregated data is generally considered more secure and therefore warrants less privacy concern as long as it is adequately aggregated.[107] For example, the CPUC exempts aggregated data that does not contain

103. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 21 (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
104. *Id.*
105. *Id.*
106. *Id.*
107. *See* SEE ACTION, A REGULATOR'S PRIVACY GUIDE TO THIRD-PARTY DATA ACCESS FOR ENERGY EFFICIENCY, at viii (2012), *available at* http://www1.eere.energy.gov/seeaction/pdfs/cib_regulator_privacy_guide.pdf ("Insight from other industries as well as historic experience of electric

PII from its privacy rules.[108] But there are concerns that as with deidentified data, external databases and reverse engineering can be used to identify private information about customers.[109] As a result, Colorado and California employ a "15/15 rule."[110] Under this rule, at least fifteen customers must be included in the data and no single customer can account for more than 15 percent of the group.[111] Alternatively, Illinois has adopted a stricter standard requiring that aggregated data must include no fewer than thirty customers.[112]

Although regulators are more willing to make aggregated data available to third parties, some risks may still need to be addressed. As reidentification practices evolve, certain sets of data previously thought to be adequately aggregated may become vulnerable. As a result, it may be necessary to adopt protocols, such as the FTC guidelines discussed above, to protect some sets of aggregated data.

It will be important for regulators to understand the various forms of AMI data and to accurately assess the privacy risks posed by each. But given the pace at which data technologies evolve, clearly delineating between each category and estimating reidentification risks for each will be a constant struggle. So regulations should focus on safeguards such as requiring companies to adhere to public attestations and contractual obligations to refrain from deanonymization attempts. These precautions allow regulators to acknowledge that the privacy risks of different types of AMI data are constantly evolving while providing means of protecting privacy and spurring innovation.

CONCLUSION

The smart grid is only just emerging. Deploying AMI is a crucial early step in achieving potential smart grid benefits. Effectively implementing these new technologies would put our nation well on its way to meeting the challenges

and gas utilities administering energy efficiency programs suggests that disclosing aggregated data poses limited risk to the customer.").

108. *See* LEE ET AL., *supra* note 49, at 1 ("Aggregated data that does not contain personally-identifiable information, is not subject to the Commission's Privacy Rules, nor is a Non-Disclosure Agreement (NDA) required to obtain such information.").

109. *See, e.g.*, *id.*

110. *See id.* at 2, 9; RUSSELL GARWACKI, S. CAL. EDISON, BIG DATA APPLICATIONS AND PRIVACY ISSUES IN CUSTOMER SERVICE, DISTRIBUTION PLANNING, AND RATE DESIGN 11 (Sept. 17, 2013), *available at* http://www.eei.org/about/meetings/Meeting_Documents/2013-09-rrac-garwacki.pdf.

111. LEE ET AL., *supra* note 49, at 9–10.

112. Investigation of Applicability of Sections 16-122 and 16-108.6 of the Public Utilities Act, Case No. 13-0506, at 4–7, 17 (Ill. Commerce Comm'n proposed Dec. 6, 2013), *available at* http://www.icc.illinois.gov/docket/files.aspx?no=13-0506&docId=206711.

faced by our aging infrastructure. Investments in AMI and AMI-enabled products and services could create a new era of consumer behavior geared towards efficiency and conservation. Utilities would be able to offer increasingly better services, and entire new sectors of the economy could be created as entrepreneurs recognize opportunities in the evolving energy arena. Finally, a range of benefits, environmental and otherwise, could be realized through reduced consumption and the introduction of clean energy technologies.

We first must take seriously the potential privacy risks associated with such a transformation. Failure to adequately tailor new policies to incorporate privacy concerns as well as potential benefits could significantly hamper the rollout of these new technologies or, even worse, result in serious backlash. By looking at the levels of risk associated with various forms of AMI data and implementing adequate safeguards, a range of policies can be developed that reinforce privacy protections without hampering the ability of the smart grid to reach its full potential.