National Regulatory
Research Institute

Smart Grid Data:
Must There Be Conflict Between Energy Management and Consumer Privacy?

Sherry Lichtenberg, Ph.D.

Principal, National Regulatory Research Institute

December 2010

10-17

Acknowledgments

The author wishes to thank Michael Jung, Bill Levis, Frank Shafer, and Joseph Witmer for their thoughtful comments and recommendations. She also wishes to thank Marjorie Conner for her research, review, and comments and Scott Hempling for his help in understanding the challenges and trade-offs facing state regulatory commissions in implementing the smart grid.

Online Access

This paper can be accessed online at http://www.nrri.org/pubs/telecommunications/NRRI_smart_grid_privacy_dec10-17.pdf.

Executive Summary

Smart grid technology promises a more efficient, reliable, useful, and cost-effective energy future. It will provide a way to track and manage our power usage in real time, better operate current grid assets, integrate forthcoming technologies (e.g., distributed generation and storage, electric vehicles), identify and implement savings opportunities, and husband scarce resources. But with this promise comes the potential for harm from loss of privacy due to poorly implemented policies governing the sharing of energy consumption data with energy providers, their suppliers, product developers, advertisers, and others who can mine this data to target and influence buying behavior. Are these privacy risks real? Are they significant enough to warrant new or revised regulations? How could the use (or misuse) of energy consumption data negatively impact consumers? And finally, are these risks outweighed by the economic, societal, and environmental benefits of the smart grid?

A. What is the smart grid and how will it impact individual privacy?

Proponents of the smart grid assert that by providing highly granular consumption data, the smart grid will benefit utilities, customers, and society by enabling more efficient "real time" energy management, encouraging the development and use of more energy-efficient appliances, and reducing peak energy usage by moving less critical activities to non-peak times. These commenters also posit that smart grid data will benefit society by increasing the reliability of the electrical system through automatic outage notification, accelerated service restoration, and improved grid asset management. They also cite environmental benefits, including reducing emissions by enhancing grid efficiency and limiting the need to build new generation, transmission, and distribution facilities by boosting system load factor and reducing peak demand. Finally, smart grid supporters point out that smart grid data will generate commercial benefits by encouraging the development of a new energy information marketplace that will provide the tools and services consumers will need to understand and manage their energy use.

As the following table shows, the granular nature of the data collected and transmitted over the smart grid and the use of this data to draw individual energy profiles has also raised concerns from consumers, consumer advocates, and state commissions about the potential negative effects of the misuse of personal data or the release of inaccurate data.

Energy Data Disclosure Concerns

Appliance Use	Activity Disclosure Risk – Low	Activity Disclosure Risk – Medium	Activity Disclosure Risk – High
Hot water heater	Washing clothes		Bathing
Washer/dryer	Washing/drying a single load		Number of loads per day/week could reveal home occupancy levels
Lights	At home and awake	Not at home – daily on/off time shows daily schedule	No usage - out of town/on vacation Extremely high usage – potential illegal activity
Microwave/stove/oven	Cooking	Shows daily work schedule	
Hair dryer		Post shower - Getting ready for work/other activity	On/off times may identify daily schedule
Dishwasher	Washing dishes		No usage for long periods may signify vacation
TV	At home and watching		On/off times may identify daily schedule
Air conditioner/heat pump	Cooling/heating schedule		On/off times may identify daily schedule
Computer	Working/surfing the net		Risk for theft
Alarm system	Home or away		
Medical equipment		Customers may not want others to know they are on oxygen, dialysis, or some other treatment regimen	Violation of HIPPA rules

Achieving the efficiency and peak period load reduction goals of the smart grid depends in large part on obtaining information from and about consumers—their usage patterns; the type, age, and efficiency of the appliances installed in their homes; the cost of their energy usage—and sharing this data with the utility, third-party suppliers, and equipment manufacturers. As smart grid proposals proliferate, regulators are focusing on the tradeoffs between consumer privacy and utility data needs, a task that requires an understanding of energy issues, privacy issues, and the smart grid itself, as well as an evaluation of existing privacy regulations.

B. What are the key issues of the smart grid privacy debate?

This paper seeks to define the key issues of this new debate.

1. Is all personal data the same, or should it be placed into categories that require different privacy treatment?

2. By what method should consumers consent to the use of their data by the utility, its affiliates, and other parties? Should the regulator assume consent simply because consumers have had a smart meter installed at their homes or have agreed to participate in smart grid programs? Is proactive consent required? Should the requirement for consent vary depending on the type of data that will be shared?

3. Who will receive any monetary rewards generated by the sale of consumer energy data?

To answer these questions, this paper examines definitions of the smart grid, identifies key components of "private information," examines why they are important to achieving the smart grid's efficiency and peak period load reduction goals, and suggests methods for meeting the needs of both utilities and customers as industry and the states move forward with smart grid deployments.

The issues in the smart grid debate are not absolutes; instead, they represent a series of tradeoffs among the types of data that must be shared, who controls that data, and who will decide when and how it will be used. The key conflicts among the various parties involved in collecting and using smart grid data include:

1. The conflict between the utility's operational needs for customer data and the customer's concern that that data will be misused or insufficiently protected.

2. The conflict between the utility's interest in using customer data to develop its own proprietary products and services versus adopting policies and technologies that facilitate competitive markets for products and services.

3. The conflict between commercial interests and consumer privacy.

4. The conflict between society's interests and consumer privacy.

C. Who should control access to smart grid data?

To resolve these issues, regulators must evaluate the benefits of smart grid data, the need for privacy, the potential for harm from inadequate data protections, and determine who should control access to individual consumer consumption data. Potential answers to these questions include categorizing the data based on its ultimate use and the potential for harm, requiring utilities to aggregate data to remove personal information, and giving consumers control of any of their own data beyond that required by the utility to install or disconnect service, make repairs, bill for consumption, and plan for new transmission, distribution, and generating facilities. In determining who should control access to consumer data, regulators should focus on three principles:

1. Decisions regarding the control and use of personal energy consumption data depend on the ultimate uses for that data. Multiple uses may require multiple decisions.

2. As a default, utilities may use individual consumption data only for commission-defined public interest purposes (i.e., to carry out their obligation to serve, such as for grid operations). Utilities may use the data for other purposes, such as to provide additional products and services, if they (a) obtain customer consent, and (b) demonstrate that they do not have an unearned competitive advantage over competing providers of such products and services. The utility should not have a right of access to the data greater than its competitors.

3. Consumers should be free to contract with utilities and third parties for the use and management of their energy data commission.

The following table provides examples of the way in which these principles can be used to guide smart-grid decisionmaking.

Competing Interests Require Multiple Solutions

Smart Grid Capability/Benefit	Value to Utility	Value to Society	Value to Consumer	Consumer Privacy Concern	Mitigation Strategy	Who Regulates?
Remote reading and billing of usage; improved performance; automated outage notification	Reduced personnel costs; increased billing accuracy and timeliness	Reduced carbon emissions (no driving); minimize time lost to power outages	Accurate and on-time billing; no need to wait for meter reader; real-time incentive to adjust usage	Information security; risk of identity theft; incorrect or incomplete information	Network security design; consumer access to and correction of data errors	Commission
Reduced demand/improved transmission planning	Reduced costs; better service	Improved environment	Reduced costs	None	N/A	Commission
Utility and consumer load management	Reduce peak demand	Reduced need for new facilities	Real-time energy management	Intrusion into energy use patterns; utility may try to control usage	Customer education; clear statement of utility and customer responsibilities	Commission
Detailed energy use profile	New products and services; reduced demand	Reduced demand	Real-time energy management; reduced costs	Personal information may be leaked to wrong doers	Customer must opt into profile development	Commercial agreement; commission enforcement of "bad acts"
Commercial product development	Enhanced revenue	N/A	Energy management solutions	Overzealous marketing	Consumers decide when and how to share data	Commercial contracts; commission enforcement of "bad acts"

D. Existing federal and state rules provide a foundation for privacy protection.

Although smart grid technologies are new to the electricity industry, the data protection and privacy issues raised by the implementation of these services are similar to those faced by other industries, such banking, on-line shopping, and telecommunications. The telecommunications industry has been addressing questions regarding consumer information privacy since Congress passed the Telecommunications Act of 1996. The Federal Communications Commission's (FCC) Customer Proprietary Network Information (CPNI) rules address privacy questions similar to those raised by the deployment of the smart grid. The FCC classifies consumer data based on the potential for harm caused by the disclosure of personally identifiable information (for example, identity theft caused by the release of account and billing

information). Its privacy rules provide a process for protecting personal data, as well as obtaining permission to use it for specific purposes such as installing and billing service or marketing service bundles. Although the CPNI rules do not specifically address all the issues raised by the smart grid (for example, providing data to third parties to manage consumer energy consumption), they provide regulators with an example of the way in which another industry has successfully adopted a regulatory approach for protecting sensitive consumer information from unauthorized release while simultaneously allowing its use for other purposes.

The National Institute of Standards and Technology's (NIST) proposed privacy evaluation process and the Federal Trade Commission's (FTC) Fair Information Practices standards also address the issue of protecting the privacy of consumer data, while allowing data sharing when required. An FTC report released in December, 2010

> proposes a framework to balance the privacy interests of consumers with innovation that relies on consumer information to develop beneficial new products and services. The . . . report . . . suggests implementation of a "Do Not Track" mechanism . . . so consumers can choose whether to allow the collection of data regarding their online searching and browsing activities.[1]

As smart grid development moves forward, commissions will be faced with determining when regulation is necessary, who should create the rules, and whether a state-specific or national smart grid privacy policy best serves public policy needs. This paper proposes a process for conducting these evaluations and developing the regulations necessary to ensure that utilities and their suppliers can collect and share the data required to achieve the benefits of the smart grid while simultaneously protecting critical consumer data from improper use. The four key components of this process are:

- Identifying the information utilities will collect, determining with whom, and for what purposes it will be shared and assessing the need for protecting that data.
- Ensuring that consumers understand what data will be shared and under what terms and conditions.
- Requiring utilities deploying smart grids to implement internal privacy training programs and customer notice procedures.

---

[1] "FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers," FTC Privacy Press Release, 12/2/2010, available at http://ftc.gov/opa/2010/12/privacyreport.shtm

- Enforcing privacy rules, regularly reviewing and evaluating utility performance, and assessing fines if applicable.

The smart grid privacy debate is just beginning, giving regulators a unique opportunity to forge a workable regulatory solution to the privacy issues involved in implementing the smart grid.

Table of Contents

I. Introduction

Utilities, environmentalists, and consumers have been asserting the benefits of a new "smart" electric grid that will allow energy users, suppliers, and equipment manufacturers to engage in a wide range of new functions, including automating distribution management (for example meter reading and trouble handling), charging electric vehicles (EV), monitoring and adjusting energy usage in "real time," shifting demand from peak periods to underutilized time slots, delaying or even canceling the need for new generating capacity, and allowing remote service installation and management. As the U.S. Department of Energy (DOE) states in its third Smart Grid Request for Information (RFI),

> The Smart Grid better integrates information, communication, and intelligent control technology, into the nation's electrical system. It will offer new tools to maintain reliability and improve flexibility. It has the potential to improve power quality, manage power scarcities and reduce transmission congestion costs. 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 security or reliability.[2]

While this vision of the future sounds like a promising way to reduce our energy consumption, it also raises questions about what information utilities and others will collect to achieve this vision and who should have access to and share the consumer consumption data generated by the smart metering infrastructure and the smart appliances connected to the network and transferred over the smart grid. As the National Association of Regulatory Utility Commissioners (NARUC) points out in its July 2010 resolution, the Smart grid "poses significant privacy issues that need to be considered and resolved by regulators" as these new services are deployed.[3]

Achieving the energy efficiency and peak reduction goals of the smart grid depends on obtaining information from and about consumers—their usage patterns; the type, age, and efficiency of the appliances installed in their homes; the cost of their energy usage—and sharing this data among the users, the utility, and, potentially, third-party suppliers and equipment manufacturers. As smart grid proposals proliferate, regulators are focusing on the tradeoffs between consumer privacy, utility data needs, and the competitive development of new energy products and services, a task that requires an understanding of energy issues, privacy issues, and the functions of the smart grid itself, as well as an evaluation of existing privacy regulations.

This paper provides a framework for defining and evaluating the key issues of this new debate.

---

[2] Federal Register, Vol. 75, No. 180, Friday, September 17, 2010/Notices, p. 57007.

[3] http://www.naruc.org/Resolutions/Resolution%20on%20Smart%20Grid1.pdf

1. Is all personal data the same, or should it be placed into categories that require different privacy treatment?

2. By what method should consumers consent to the use of their data by the utility, its affiliates, and other parties? Should the regulator assume consent simply because consumers have had a smart meter installed at their homes or have agreed to participate in smart grid programs? Is proactive consent required? Should the requirement for consent vary depending on the type of data that will be shared?

3. Who will receive any monetary rewards generated by the sale of consumer energy data?

As the first step in balancing the needs of the competing interests in the smart grid privacy debate, this paper defines the smart grid, identifies the key components of "private information," examines why they are important, and suggests methods for meeting the needs of both utilities and customers as industry and the states move forward with smart grid development. This paper is directed at regulators and staff engaged in smart grid approvals and consumer protection. While it presupposes a basic understanding of electricity regulation and data collection, the paper is geared to all parties in the debate about consumer privacy and energy self-sufficiency.

Part I of this paper introduces the questions that must be considered by regulators in addressing smart grid privacy issues.

Part II defines the smart grid and identifies the types of data that will be generated by customers, transmitted over the smart grid, and used by utilities and third parties to create energy profiles, manage individual energy usage, and develop and market new products. It also addresses the question of what makes some consumption data private and identifies the potential harms associated with energy usage profiling and the unregulated release of personal information.

Part III reviews the analyses necessary to construct regulatory solutions that will ensure that the benefits of the smart grid are realized without unnecessarily compromising consumer privacy. This section identifies the sometimes opposing positions on data ownership and control held by those who generate the data and those who want to use it. It also discusses potential principles for controlling the release of personal data, including its sale or transfer to third parties.

Part IV reviews existing rules for protecting personal information from other entities, including the Federal Communications Commission's (FCC) Customer Proprietary Network Information (CPNI) rules for common carriers and the Federal Trade Commission's (FTC) privacy principles. This section also addresses the rules developed by those states that have already created strategies for using customer information productively while protecting customer privacy.

Part V provides regulators with recommendations for reconciling the disparate interests of utilities, consumers, and third party product developers in order to resolve the privacy issues raised by smart grid deployment.

Part VI is the conclusion.

II. What Is the Smart Grid and Why Do We Need to Consider Its Impact on Privacy?

In this section of the paper, we consider definitions of the smart grid, identify the data that will be carried over it, and determine what makes this data private. We also examine the potential value of smart grid data and discuss ways to protect it, control it, and benefit from it.

A. What is the smart grid?

Most current definitions for the smart grid focus on what it "does" and are functional rather than prescriptive or descriptive. For example, as part of the Energy Independence Act of 2007,[4] Congress instructs the U.S. Department of Energy to manage the deployment of a smart grid, whose functions will include:

> (1) The ability to develop, store, send and receive digital information concerning electricity use, costs, prices, time of use, nature of use, storage, or other information relevant to device, grid, or utility operations, to or from or by means of the electric utility system, through one or a combination of devices and technologies.
>
> (2) The ability to develop, store, send and receive digital information concerning electricity use, costs, prices, time of use, nature of use, storage, or other information relevant to device, grid, or utility operations to or from a computer or other control device.
>
> (3) The ability to measure or monitor electricity use as a function of time of day, power quality characteristics such as voltage level, current, cycles per second, or source or type of generation and to store, synthesize or report that information by digital means.
>
> (4) The ability to sense and localize disruptions or change in power flows on the grid and communicate such information instantaneously and automatically for purposes of enabling automatic protective responses to sustain reliability and security of grid operations.
>
> (5) The ability to detect, prevent, communicate with regard to, respond to, or recover from system security threats, including cyber-security threats and terrorism, using digital information, media, and devices.
>
> (6) The ability of any appliance or machine to respond to such signals, measurements, or communications automatically or in a manner programmed by its owner or operator without independent human interventions.

[4] *Section 1306(d) of the Energy Independence and Security Act of 2007*, Pub. L. No. 110-140, 121 Stat. 1492 (2007)

(7) The ability to use digital information to operate functionalities on the electric utility grid that were previously electro-mechanical or manual.

(8) The ability to use digital controls to manage and modify electricity demand, enable congestion management, assist in voltage control, provide operating reserves, and provide frequency regulation.

(9) Such other functions as the Secretary [of Energy] may identify as being necessary or useful to the operation of a smart grid.

In "A Briefing Note from the Department of Engineering and Public Policy," published in 2009,[5] a Carnegie Mellon University study proposes that we look at the smart grid in terms of its benefits to key users: (a) the customer, who will receive the benefit of automated meter reading and time of day/time of use pricing; (b) the distribution system, which will be automated and have selective load control; and (c) the transmission system, which will include advanced measurements of power flow and advanced devices for managing that flow.

The Ontario (Canada) Parliament provides this definition in a 2009 amendment to the Electricity Act of 1998.

> For the purposes of this Act, the smart grid means the advanced information exchange systems and equipment that when utilized together improve the flexibility, security, reliability, efficiency and safety of the integrated power system and distribution systems, particularly for the purposes of, (a) enabling the increased use of renewable energy sources and technology, including generation facilities connected to the distribution system; (b) expanding opportunities to provide demand response, price information and load control to electricity customers; (c) accommodating the use of emerging, innovative and energy-saving technologies and system control applications; or (d) supporting other objectives that may be prescribed by regulation.

In this paper, we recommend thinking about the smart grid as the electric transport analogue to the public switched telecommunications network (PSTN)—a self-healing, ubiquitous grid that includes both devices (e.g., physical energy delivery infrastructure, digital appliances and other endpoints, and the network communications that connect devices) and applications (e.g., information acquisition and presentation, the control of energy production, delivery, and consumption), passes data among multiple points, and allows "real time" observation, storage, and management of that data.[6]

---

[5] M. Granger Morgan, Jay Apt, Lester B. Lave, Marija D. Ilic, Marvin Sirbu, and Jon M. Peha, The many meanings of "Smart Grid"; Carnegie Mellon Department of Engineering and Public Policy, Carnegie Mellon University, June 2009.

[6] Different commenters interpret "real time" differently; some think data should be provided in less than 1 second; others suggest that less than 10 seconds or even less than a

B. The smart grid will enable utilities and others to collect a range of personal information from consumers

The collection of customer data concerning electricity usage is not new. Utilities have always collected and protected information about their customers, and those customers' energy use, in order to bill for monthly power consumption, estimate potential demand, and plan and design the electric grid. This data has included the number of kilowatt hours (kWh) an individual customer uses on a monthly basis and over time, the physical location of the customer's meter, and the customer's bank account, credit card, and payment history information. Meter readers have often had to enter the customer's physical premises to gain access to the meter to read it or start or stop service. But prior to the advent of smart meters and the smart grid, the data gathered from electric meters has been used for a single purpose--to calculate the number of kWh used and generate the customers' bill. Because this billing data was collected monthly in arrears and was used for a single purpose, the risk to consumer privacy was minimal.

The smart grid adds another layer of customer-specific information to the data utilities will collect. With the smart grid and the array of smart meters and smart appliances it brings with it, utilities will be able to collect not just the billing and account data that they have gathered in the past but more detailed information regarding customers and their energy use, someday down to the individual appliance and activity level. In addition, the smart grid will allow utilities to gather and transmit information about consumer energy usage in "real time," as that information is created.[7]

Each time we turn an appliance or the lights on or off, raise or lower our thermostat, or run hot water in the shower, we make a request to the electric company for power. Each of these requests is an event that could be used to create an individual energy profile. As Elias Quinn points out in his study on smart grid privacy for the Colorado Public Utilities Commission, once the smart grid is fully deployed (and the customer has purchased appliances capable of "smart" communications), utilities will be able to collect detailed information about their customers, including:

1. Time of day, day of week, day of month an appliance is turned on or off and the length of time that appliance is used;

---

minute is fast enough. The Colorado Smart Grid task force is also discussing whether "real time" means 1 minute, 5 minutes, or some other time factor.

[7] Even without "smart appliances," utilities have already implemented programs that allow them to control when and at what times consumers use large-demand appliances such as air conditioners or heat pumps in order to reduce demand during peak periods. See http://www.nwcouncil.org/energy/dr/library/dlf_waterheat.pdf; http://repository.tamu.edu/bitstream/handle/1969.1/6651/ESL-HH-94-05-31.pdf?sequence=4; http://www.kema.com/services/consulting/utility-future/smart-grid/load-control.aspx; https://supplier.bge.com/LoadProfiles_EnergySettlement/ALM.htm.

2. The number of simultaneous electrical devices in use at one time ;

3. Amount of energy used per transaction and the total amount of energy used over the billing period;

4. The cost of the energy used for each transaction (i.e., the discrete cost of turning on and using a specific appliance); and the

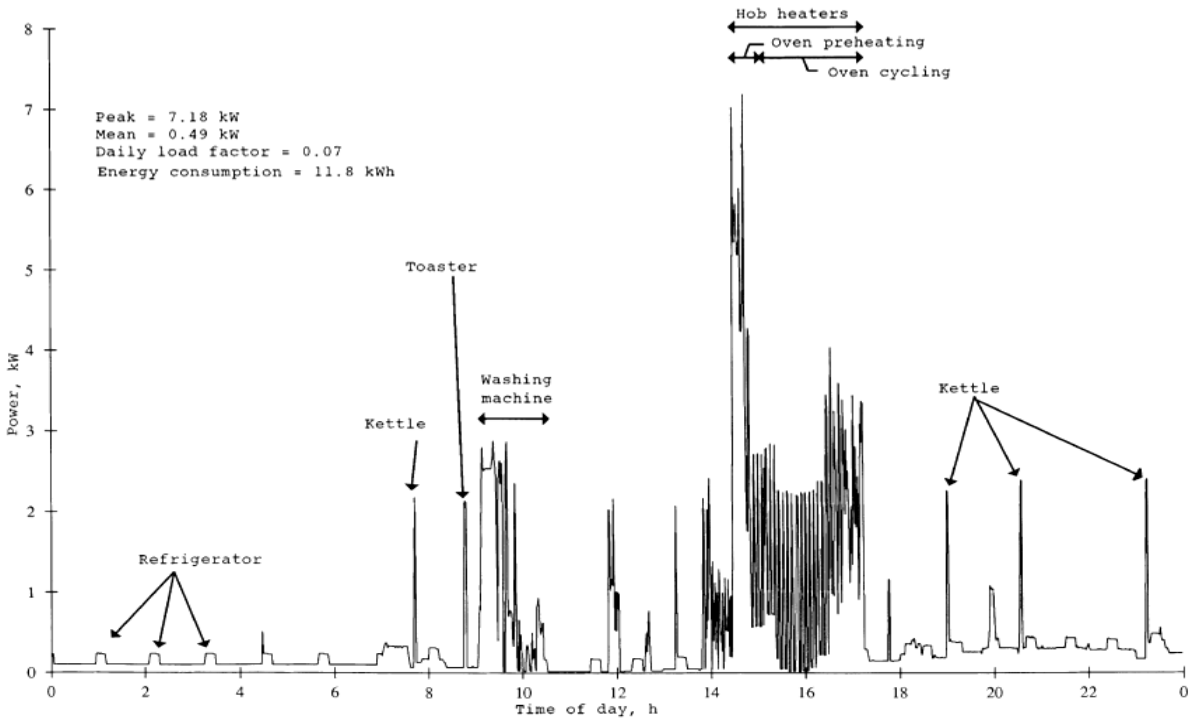
5. Type of appliance being used (i.e., hairdryer, washing machine, water heater).[8]

Each event will generate data that the utility can use to manage load, shift usage, or determine how scarce generation, transmission or distribution capacity should be allocated; that customers can use to review and manage their own energy consumption; and that third party vendors may use to develop and market new, energy efficient appliances and software applications to manage those appliances.

With this new technology, utilities, consumers, and third parties can use energy transaction data to create individual energy profiles. Quinn's diagram of the information about an individual user's energy profile shows the personal information that can be obtained by analyzing the data transmitted over the smart grid:[9]

[8] Quinn, Elias L., *Smart Metering & Privacy: Existing Law and Competing Policies, A Report for the Colorado Public Utilities Commission*, Spring 2009, pages 1-2.

[9] Ibid.



This diagram shows the energy usage of a single household over a 24-hour period. During the hours after midnight, when the resident is asleep, the refrigerator works at its normal level, but other appliances are unused. A spike occurs just before 8 AM when the tea kettle and toaster are used to start breakfast. Additional spikes point to the washing machine, the dryer, and the oven preheating for dinner. Energy usage moderates until the end of the day, when the homeowner presumably has his last cup of tea and goes to bed.

In the long term, sophisticated, "smart" appliances with radio frequency interface (RFI) chips will communicate with smart meters, the utility, equipment manufacturers, and others to provide an even more detailed picture of a user's life. "Smart" appliances will identify themselves to the grid the way cell phones register themselves on the mobile network today, providing information about where, when, and how they are being used. Electric cars will provide information about customer driving habits and locations. As Pacific Gas and Electric points out in an article in the San Francisco Examiner, "Smart-grid technology is being developed to help cars communicate with the utility when they are plugged in. We need to know that a car is charging, how long it needs to charge and how we can balance that so that we don't tax the wires or the transformers."[10]

It is the customer-specificity of the "energy transaction data" captured via the smart grid and its potential uses by the utility, the customer, and third parties that has launched the debate over privacy and the smart grid. According to comments filed with the DOE on its Request for Information (RFI) on the need for energy privacy rules:

[10] *San Francisco Examiner*, 4/18/2010, http://www.sfexaminer.com/local/Electric-cars-searching-for-a-place-to-plug-in-91080329.html

> A survey commissioned by Edison Electric Institute (EEI) found that consumers place a very high priority on privacy. Forty-six percent of respondents believe that it is very important for their electric usage data to be kept confidential, and 29 percent believe it is somewhat important, while 79 percent believed that only utilities and customers should have access to smart meter information.[11]

C. The personal data collected by the smart grid will produce benefits and risks.

Proponents of the smart grid assert that the data collected via the smart grid will benefit individual consumers, utilities, and society as a whole. With the "real time" information provided by the smart grid, consumers will be able to evaluate and modify energy usage based on their own specific requirements and appliances. Utilities will obtain clearer and more specific data with which to plan long term generation and distribution needs, develop pricing plans, and provide customers with incentives to use power at off peak times. "Real time" energy usage information may also benefit equipment manufacturers (and thus the economy as a whole) by helping customers to see how replacing existing equipment with more energy efficient appliances will reduce usage and lower costs. And, finally, the data provided by the smart grid could create new markets for information technology companies that will create customer software to allow the tracking and modeling of energy usage information.

But the data from the smart grid can also have negative impacts on individual consumers by allowing the creation and inappropriate sharing of detailed energy profiles. The following paragraphs describe both the benefits and the risks of smart grid data collection and their impact on consumer privacy.

1. Benefits to consumers, utilities, commercial enterprises, and society

a. Consumer benefits

Because information from the smart grid will be transmitted in "real time," as it is collected[12] rather than simply as a line item on a bill provided at the end of the month, the smart grid can involve customers in managing their own energy use, creating both the incentive to limit and/or shift energy demand and giving them the tools they need to do so. Smart grid data will allow customers to (1) shift usage from peak times to periods of lower demand; (2) review energy costs in "real time"; (3) benefit from lower, off-peak usage rates; (4) identify the need for more energy efficient appliances, and (5) even manage their appliance use remotely.

As Google points out in the advertising for its PowerMeter software, the smart grid will allow customers to capture, review, and manage their own energy costs prior to receiving a bill

[11] NETL Smart Grid Implementation Strategy: Understanding the Benefits of the Smart Grid v1.0, p.28

[12] Companies differ on whether data needs to be provided immediately, in short increments, or over a longer period of time, but the majority of commenters agree that the more immediate the data, the greater the likelihood that customers will use it to modify their energy use.

by accessing this information on-line from the utility's data base or via a third-party software package like Google PowerMeter,

> a free energy monitoring tool that helps [consumers] save energy and money. Using energy information provided by utility smart meters and energy monitoring devices, Google PowerMeter enables [consumers] to view [their] home's energy consumption from anywhere online.[13]

In the long term, according to appliance manufacturers and those planning to develop third party energy management systems, information on the energy demand of individual appliances will encourage customers to evaluate the way in which they use those appliances, shifting usage to lower cost time periods, suspending or modifying high cost activities or choosing alternate processes, like hanging out the wash rather than using the dryer, in order to lower costs, save energy, and improve the quality of the environment. Manufacturers like General Electric have already begun describing "smart" clothes dryers and other appliances that will be able to communicate with the utility and the customer to determine when the timing is right to begin the drying cycle. These companies have also described other "smart appliances" that will use energy data to notify customers when their appliances are working at less than peak efficiency, need to be replaced, or can be modified to draw smaller amounts of power.[14]

Utilities also cite the consumer benefits of the smart grid in their applications to deploy the "smart meters" used to implement the grid. For example, the Baltimore Gas and Electric application for a "tracker tariff" to pay for smart meter installation pointed out that,

> in addition to conserving energy and reducing energy costs, the Smart Grid Initiative will provide for significant customer benefits and operating and capital savings. These customer benefits include: greater efficiencies with regard to meter reading, handling of service orders, management of outages; enhanced customer service capabilities and quicker resolution of billing issues due to access to real-time meter data; and access to detailed consumption data to assist customers in managing their energy usage to give them the opportunity to save on their energy bills.[15]

---

[13] http://www.google.com/powermeter/about/about.html While the PowerMeter software is currently free, as smart metering and smart grid initiatives expand, companies will develop a competitive market for this type of software product and the web storage required to archive and manipulate this data.

[14] See http://articles.cnn.com/2009-07-16/tech/cnet.smart.grid_1_smart-grid-technologies-smart-grid-smart-meters?_s=PM:TECH

[15] *Application of Baltimore Gas and Electric Company for Authorization to Deploy a smart Grid Initiative and to Establish a Surcharge Mechanism for the Recovery of Costs* Maryland PSC, Case Number 9208 (8/13/10).

The smart grid will also provide customers with indirect benefits. Since utilities will read smart meters remotely and customers will be able to check their billing any time they want, estimated bills will be largely eliminated, and customers will have the ability and the incentive to budget their usage, particularly during the most expensive heating and cooling months. They may also have fewer questions regarding their bills, since they will be able to monitor their consumption throughout the month, ultimately reducing calls to utility service lines over the long term. And, finally, because the grid will report its status to the utility on a regular basis, outages will be reported and repaired more rapidly and may even be reduced in frequency and duration as the enhanced reporting capability of the equipment in the network improves grid reliability, preventive maintenance scheduling, and distribution asset management.

b. Utility system benefits

Utilities will benefit from the smart grid through reduced costs and enhanced service. The smart grid will provide utilities with "real time" information about the way in which the power they generate and distribute is being used. This data will allow them to:

1. Know what appliances are being used and at what time during the day so they can plan and manage loads more efficiently;

2. Capture information on customer equipment upgrades, allowing them to calculate rolling forecasts of energy use;

3. Adjust the temperature of a customer's home or turn off heating and cooling systems or other large appliances during peak periods, reducing the potential for system overloads and brownouts or blackouts;

4. Reduce staff levels by reading meters remotely rather than dispatching personnel to customer locations;

5. Install or disconnect electricity service remotely, reducing the losses from un-paid bills and limiting the need for dispatching personnel to customer locations.[16]

c. Commercial benefits

The smart grid and the data it provides will create new consumer and business markets. Prior to the smart grid, energy usage data was of interest only to the customer and her utility. Utilities used the data for billing and planning purposes. Customers who wanted to manage their usage could compare the data from their bills to see whether their use was higher or lower than the month before. They could limit or eliminate the use of various appliances to reduce usage but had to wait for the next month's bill to understand the impact of those actions. The review

---

[16] The consequences of the remote disconnection of meters have already begun to concern some regulators. See Illinois Statewide Smart Grid Collaborative, p 146, http://www.ilgridplan.org/default.aspx

process was manual and did not take into account usage impacting activities like vacations, cold spells, or heat waves.

The smart grid brings customers "real time" energy management capabilities and may provide new commercial opportunities for utilities, their subsidiaries, and third party energy management companies. Companies like Google and Cisco are already developing products to help end-user customers manage their energy use, while giving utilities the tools they need to collect and manage data from the smart grid. As Google points out in its response to the California Public Utility Commission's rulemaking on smart grid technology (RO8-12-009):

> Third party service providers [will] offer the means to better engage consumers by making data available to them in ways that can be integrated into the[ir] daily lives . . . For example, a third party provider could offer consumers a service that analyzes energy use, identifies inefficient appliances, provides appliance discounts or suggests energy management practices.[17]

As implementation of the smart grid expands, other third party marketers and equipment makers will use customer data to determine the age of an appliance and provide targeted advertising aimed at selling new or more energy efficient equipment, develop mobile applications for operating home appliances remotely depending on the customer's current level of energy usage, and create other new applications. Suppliers are already describing Home Area Networks (HANs) that will allow consumers connect "plug and play" smart appliances from a variety of vendors to the smart grid networks through which their smart meters are communicating. Using Internet access, where available, customers will be able use emerging "smart grid web portals" to access their consumption information, download information from the utility's computers to create graphic displays of energy usage, and evaluate the impact of new purchases or model the costs associated with using different appliances at different times.

As energy information becomes a commodity to be sold or traded on the open market, utilities and consumer advocates are raising the question of ownership and control.

On one side of the debate are those who claim that because the utility provides the smart meter, it owns the customer's data and can use it for applications beyond the traditional roless of billing and grid operations, even without customer consent. For example, the National Rural Electric Cooperative Association (NRECA) posits that

> if a utility or its agent purchases and installs an advanced meter in order to collect data required to bill for electric service and to monitor the condition and performance of the distribution system, then the utility owns the data it collects.[18]

---

[17] *Comments of Google Inc On Proposed Policies and Findings Pertaining to the Smart Grid Policies Established by the Energy Information and Security Act of 2007*, http://www.google.com/powermeter/about/cpuc.html

[18] National Rural Electric Cooperative Association, *Comments on DOE NBP ROI*, July 12, 2010.

The National Association of State Utility Consumer Advocates (NASUCA) takes an opposing position. In comments to the U.S. DOE., NASUCA states that consumers both generate the data transmitted over the smart grid and pay for the meters that transmit it (via their electric rates). Therefore, NASUCA asserts,

> the customer must own her or his home energy usage data, have consistent access to that data for personal review in a usable format, be fully informed of what data is flowing to and from the meter, to whom the data is flowing, and with what frequency the data is communicated.[19]

Over the long term, regulators will need to determine who should receive any monetary compensation derived from the sale of smart grid data, through what process, and with what constraints and procedures.[20] We discuss possible principles for making those decisions in Section III.

d. Societal benefits

The U.S. DOE summarizes the societal benefits of the smart grid in the introduction to the National Energy Technology Laboratory's study:

> By far, the biggest winner [from the implementation of the smart grid] will be society as a whole. The smart grid is expected to provide benefits to society in the following areas:
>
> - Reduced losses to society from power outages and power quality issues
> - Improved operating efficiencies of delivery companies and electricity suppliers
> - Improved national security
> - Improved environmental conditions
> - Improved economic growth[21]

---

[19] Comments of NASUCA, *US DOE RFI, Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy* (July 12, 2010).

[20] The monetary compensation derived from the sale of individual smart grid data is separate from the financial benefits utilities will receive from reductions in personnel and other costs due to automating current manual processes such as meter reading.

[21] *Smart grid Implementation Strategy: Understanding the Benefits of the Smart Grid* v1.0 Page 2; DOE/NETL-2010/1413, July 18, 2010

As the smart grid replaces the aging, manually operated, analog electric infrastructure with new, two-way, digital communications capabilities, utilities will be able to monitor the health of the grid proactively, allowing them to repair pending faults in advance and avoid outages. The grid will report power outages automatically and accurately, allowing utilities to roll trucks to fix, rather than find, outages. Creating new, open standards[22] for sharing information across the grid will increase the ability to create new energy exchange markets and improve existing ones. By sharing information and applications, utilities will be able to improve service delivery.

Reductions in usage driven by smart grid pricing structures that reward customers for using electricity when it is most available will lower overall power consumption, limit the need to build new power plants, and reduce emissions. Remote meter reading and service installation and disconnection will limit utility site visits, reducing vehicle-based carbon emissions by limiting unnecessary driving.

Reduced consumer demand will have a significant impact on the environment and thus society as a whole. As Google pointed out in its testimony to the California PUC regarding smart grid development, giving consumers and power companies the tools to review and monitor power use can have significant impacts on the environment and the country's dependence on foreign oil.

> Studies show that when consumers can see in real time how much energy they are using, they save 5 to 15 percent on their electricity use with simple behavioral changes, and even more with investments in energy efficiency. The average U.S. residential customer spends about $1,200 a year on electricity, so savings simply based on a real-time feedback monitor could amount to $60 to $180 per year. In fact, if just half of American households cut their demand by 10 percent, the CO2 emissions avoided would be equal to taking approximately eight million cars off the road. [23]

Finally, the tools provided by an enhanced utility grid will provide the infrastructure necessary to support renewable generation from wind and solar power applications.

The DOE summarizes these benefits as follows:

> … [T]he benefits of Smart grid implementation as set forth by DOE's Modern Grid Strategy are too fundamental and enduring to ignore. Among these are downward pressure on electricity prices made possible by marketplace efficiencies and consumer involvement; improved reliability and significant

---

[22] Open standards allow product and service developers to create applications that can be used across networks, thus reducing the need for specialized personnel or computer software, increasing efficiency, and allowing the best practices of different companies to be shared.

[23] *CAPUC Proceeding RO-8-12-009, Comments of Google, Inc.* See http://www.google.com/powermeter/about/cpuc.html#feb9

outage reduction; increased grid robustness for improved grid security; reduced losses and emissions; the integration of renewable energy; substantial job growth in areas from PV installation to grid-assisting technologies; and the opportunity to revolutionize not only the utility sector, but also the transportation sector through the integration of electric vehicles as generation and storage devices.[24]

e. Personal privacy risks

Privacy is about intent, expectation, and behavior.[25] Does a consumer intend to share data about her energy usage beyond that required for the utility to bill for energy use? Does she expect that the utility will use the data for purposes beyond customer billing or that it may share the data with its own "energy management" affiliates, a third party vendor or an equipment manufacturer? Did she knowingly give her "consent" to do so? How would the knowledge that personal consumption data beyond that currently used by the utility for its traditional purposes might be shared with others transform her behavior? Regulators must answer these questions in order to develop a coherent energy data privacy policy.

Data transmitted over the smart grid can be innocuous, or it can provide a window into consumers' daily lives that could lead to adverse consequences. The positive goals of consumer and utility energy management must be balanced with the risk that this data could be misused or fall into the wrong hands. Table 1 shows how the same data can lead to multiple conclusions about private behaviors, raising different levels of concern about disclosure.

[24] *What the Smart Grid Means to You and the People You Represent*, prepared for the U.S. Department of Energy by Litos Strategic Communication under contract No. DE-AC26-04NT41817, Subtask 500.01.02, available at http://www.oe.energy.gov/DocumentsandMedia/Regulators.pdf.

[25] The Merriam Webster dictionary defines "private" as (a) for or restricted to the use of a particular person, group, or class (a private park) (b) belonging to or concerning an individual person, company, or interest (a private house) (c) restricted to the individual or arising independently of others. See http://www.merriam-webster.com/dictionary/private

Energy Data Disclosure Concerns

Appliance Use	Activity Disclosure Risk – Low	Activity Disclosure Risk – Medium	Activity Disclosure Risk – High
Hot water heater	Washing clothes		Bathing
Washer/dryer	Washing/drying a single load		Number of loads per day/week could reveal home occupancy levels
Lights	At home and awake	Not at home – daily on/off time shows daily schedule	No usage - out of town/on vacation Extremely high usage – potential illegal activity
Microwave/stove/oven	Cooking	Shows daily work schedule	
Hair dryer		Post shower - Getting ready for work/other activity	On/off times may identify daily schedule
Dishwasher	Washing dishes		No usage for long periods may signify vacation
TV	At home and watching		On/off times may identify daily schedule
Air conditioner/heat pump	Cooling/heating schedule		On/off times may identify daily schedule
Computer	Working/surfing the net		Risk for theft
Alarm system	Home or away		
Medical equipment		Customers may not want others to know they are on oxygen, dialysis, or some other treatment regimen	Violation of HIPPA rules

The National Institute of Standards (NIST) categorizes the information that will be generated and transmitted by the smart grid as personally identifiable, physical and behavioral.[26]

1. **Personally identifiable information**. Information that can be used to identify a person directly or indirectly, for example, social security number, billing account number, telephone number, address, and similar information.[27]

[26] *NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0* – Aug 2010, pg. 6

[27] This definition is similar to that used by the FCC in defining what it refers to as customer proprietary network information (CPNI).

2. **Physical information**. This category "covers such things as physical requirements, health problems, and required medical devices."[28]

3. **Personal behavior**. This category includes the activities consumers perform inside their homes, from washing dishes to watching TV.

Each of these categories represents a different level of concern about consumer privacy, from the revelation of key identification information to information on what a consumer does when she is inside her home. As the NIST study points out:

> A detailed sense of activities within a house or building can be derived from equipment electricity signatures, individual appliance usage data, time patterns of usage, and other data [and] can provide a basis for potentially determining [information] about occupant activities and lifestyle . . . [including] the number of individuals at a premise, when the location is unoccupied, sleep schedules, work schedules, and other personal routines.[29]

Depending on how the information collected by smart appliances and the smart grid is combined and used, it can reveal enough about a user's daily life to cause personal risk. The two hypothetical profiles that follow show how the collection of energy consumption data could affect an individual consumer.

Scenario 1: Smart grid data can lead to positive changes in energy consumption.

Monitoring Patricia Doe's Smart Meter reveals her daily routine. Patricia comes home from work at 6 pm. The electricity usage from her heat pump rises. (Her dual setback thermostat has changed the temperature in her house.) Her microwave causes another energy event (she's cooking dinner). The dishwasher turns on at 9. She takes a bath at 10 (the electric hot water heater is working). She goes to sleep at 11. (Energy usage drops.) She wakes at 6, showers, styles her hair (her hairdryer is not energy efficient; usage spikes), and leaves the house at 8. (Energy use falls).

The data generated by Patricia's energy use is transmitted to the utility on a real-time basis. Although it is primarily used for billing and load management, the data is also made available for a number of other uses. It could be sold to an appliance manufacturer, who will offer Patricia a reduced price on a new, energy efficient hot water heater. It could be sold to a marketing firm, who will send Patricia coupons for dishwasher detergent over her cell phone at 9 PM each

[28] The smart grid will also be able to identify medical devices that are in use the home such as oxygen concentrating machines, home dialysis machines, and other equipment, potentially leading to additional requirements for information protection covered under HIPAA guidelines.

[29] *NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0* – Aug 2010, p. 29

evening. Or it might even go to a personal products company who will send coupons for bath salts.

Scenario 2: Smart grid data can cause personal harm.

But what if the people monitoring Patricia's data use are not doing so with the best of intentions? What could happen then?

Constructing an energy profile by accessing Patricia's usage data by tapping into the utility's transport network, a team of burglars knows when Patricia leaves her house and returns home. They identify whether she is on vacation or simply out for the day and target her for robbery. Because they have identified the appliances in her house from their energy signatures, they know exactly what there is to steal. They break in, take her valuables, and are gone before anyone knows they have been there.

While this second scenario may be exaggerated, we paint it here to show the uses for energy profile data beyond simple demand management and the risks that uncontrolled use could create. Monitoring Patricia's electricity usage to create an "energy profile" that can be translated into a "personal profile" could allow Patricia and others on the smart grid to be targeted by wrongdoers.

The challenge for utilities, consumers, and regulators is balancing the potential usefulness of energy profile information with the risk associated with revealing what otherwise would be considered private.

III. What Analyses Are Necessary to Design Regulatory Solutions That Will Benefit Consumers, Utilities, and Society at the Least Cost to Privacy?

The smart grid changes the paradigm for recording, transmitting, and using energy consumption data. As the NIST task force on privacy points out, prior to the smart grid,

> [e]nergy consumption patterns [had] historically not risen to the level of public concern given to financial or health data because (1) electrical meters had to be physically accessed to obtain usage data directly from buildings, (2) the data showed energy usage over a longer time span such as a month and did not show usage by specific appliance, and (3) the utilities were not sharing this data in the ways that will now be possible with the Smart Grid.[30]

As utilities begin to collect and monitor real time consumer energy use, create energy consumption profiles, and work with third party companies to create markets for energy consumption data, the question of who will control, protect and use this information has become a critical path item for smart grid acceptance. Regulators, consumer advocates, utilities, and customers find themselves faced with the need to weigh benefit against potential harm; the control of data against open access; and commercial value against perceived "ownership."

As the Energy Privacy Information Center (EPIC) points out in its comments on California's smart grid plans, the privacy implications of smart grid technology will expand as the grid continues to grow, further challenging regulators.

> Smart grid systems will be multi-directional communications and energy transfer networks that enable electricity service providers, consumers, or third party energy management assistance programs to access consumption data. This information will go farther than the local utility. Indeed, if plans for national or transnational electric utility smart grid systems [go forward] as currently proposed these far reaching networks will enable data collection and sharing across platforms and great distances.[31]

Regulation is necessary when private interests diverge from the public interests—in this case, when consumer concerns about protecting their individual energy usage data conflict with the need to share that data in order to achieve the societal benefits of the smart grid. Because data from the grid will eventually reach beyond the individual consumer and her utility, the question

---

[30] NISTR 7628, p 9

[31] *Comments of the Electronic Privacy Information Center on CAPUC Proposed Decision Adopting Requirements for Smart Grid Deployment Plans Pursuant to Senate Bill 17, Rulemaking 08-12-009*, 6/110/10.

of what data will be shared, when, with whom, and under what rules becomes central to making decisions about privacy.[32]

Indeed, as this data is shared more widely, it will go beyond the confines of the regulated utility to other companies not subject to state commission rules. Commissions will thus also need to address methods for ensuring that customers understand the ultimate use for their energy data and how they can protect it from misuse by other entities.

The challenge for regulators is creating a structure that will align these competing interests.

This section discusses the analyses regulators might undertake and the principles they might use to use to balance the requirement for access to smart grid data with personal privacy.

A. Categorizing usage data can reduce the potential for compromising personal privacy without sacrificing the benefits of the smart grid.

In Part II of this paper, we postulated that the potential harm to consumer privacy from the inappropriate use of data collected by the smart grid results not from the data itself but from combining that information to create individually identifiable energy user profiles – and allowing access to those profiles by entities whose motives conflict with the consumers' needs or wishes. We can minimize this risk by categorizing energy consumption information based on data source, potential harm, and who needs access for what purpose. We can then create specific privacy guidelines for each data category.[33] We can further reduce the risk of harm by informing customers of the uses for the data collected by the smart grid and seeking their approval for access where privacy interests are large.

Creating energy use data categories will also allow us to determine who should have access to energy usage data, in what form, for what purpose, and subject to what constraints or procedures. Potential data categories include: (1) personally identifiable information such as name, billing address, payment history, and other account information; (2) billing data, such as amount of energy used and time of use; (3) operational data used by the utility for optimizing grid performance and monitoring and managing service quality; and (4) individual "event" data, such as what appliances a customer uses and at what times.

We can also categorize consumption information based on where it is collected; for example, is the data collected outside the home (on the utility side of the electric meter) or inside the home (on the customer appliance side of the meter). This type of segmentation would protect

[32] While consumers expect their utility to use consumption data to bill for monthly usage, unless their service contract specifically authorizes using that data for other purposes, its internal release and use by the utility and its affiliates should be treated in the same way as the release to any other third party.

[33] The FCC customer information privacy rules segment data in this way. These rules are discussed in more detail in Section IV.

customers from the potential release of information regarding the specific appliances they use, including medical equipment.

The following table summarizes how energy data might be categorized to determine the risk of harm from its release.

Smart Grid Data Can Be Categorized to Protect Private Data

Category	Data	Purpose for Collecting	Potential Harm	Who Authorizes Use
Customer identifiable information	Name, address, account number, banking or credit information	Establish utility billing account	High – identity theft, unauthorized bank account/credit card use	Consumer – part of standard service contract
	Monthly usage data, historical usage data	Customer billing Utility resource planning	Low – standard billing protections should apply	Consumer Utility
	Appliance "event" data	Manage appliance use (consumer, utility, third party)	Medium – energy use profiling	Consumer
Aggregated data	Usage by neighborhood, block, etc., stripped of identifiable information	Evaluate usage patterns Create marketing campaigns Evaluate smart grid success	Low – individual users can't be identified	Commission Consumer opt-in or opt-out program
Subscriber list	Names, addresses by program	Target marketing	Medium – could reveal subsidy or income information	Consumer opt-out

1. Data can be categorized based on purpose or potential to cause harm.

Utilities require individual consumer data and account information to bill energy usage, manage the network, identify problems, and plan for long term demand. On the one hand, the utility already collects and protects this data—the smart grid merely automates an existing process—so no scrutiny beyond that already applied to billing data is needed. On the other hand, additional scrutiny by regulators and, potentially, rules for customer consent may be required should the utility want to share this information with others.

Providing individual appliance use information to others or using this data internally to develop and market new services or products falls into a different category. The utility does not require this information to manage its network, install service, or make repairs, but could

develop a competitive advantage by restricting the sharing of customer consumption pattern data only with its own affiliates or other companies it selects.

Once we select a process for segmenting energy consumption data, we can assign a level of potential harm to its disclosure and determine how best to authorize its release. This process for intersecting policy goals with privacy goals is used in other industries where the customer's supplier collects personal information that could be used for multiple purposes but requires specific authorization for revealing that data outside the confines of its internal activities. For example, FCC's data privacy rules segment the information telecommunications carriers obtain from their customers based on the risk of disclosure of personally identifiable information. Under the FCC rules, personally identifying data may be used only by the carrier who provides the customer with service and then only for specific purposes, such as billing, installing new service, and repairing service outages.[34]

2. Aggregating information can make it "safe" to share.

Private data can be made available for public uses by removing or masking personally available information. Energy usage data can be aggregated and stripped of identifying information such as house number or account number before it is used. For example, utilities might use aggregated consumption data to shift usage away from peak periods. Third parties could use the data to create neighborhood-level energy use profiles for marketing campaigns, and regulators could use the data to evaluate the success of smart grid implementations. Regulators can address aggregated information in a number of ways: (1) approve the use of aggregated information generally without customer permission, (2) require utilities to create a process for obtaining customer permission proactively (consumer opt-in to sharing their data in an aggregated form), or (3) require utilities to inform customers of the potential uses for aggregated information and provide a process to allow customers to choose not to participate.

B. What principles can regulators apply in determining who should control the release and use of personal energy data?

Regulation is about performance; regulatory decisions must align private behavior with public need.[35] The multiple interests in the smart grid privacy debate increase the challenge for regulators, who must manage the trade-offs between the risk to personal privacy from sharing data about individual energy use with the benefit to society as a whole from encouraging

[34] Personally identifiable information may also be provided to law enforcement after receipt of a properly executed subpoena. We discuss the FCC data privacy rules in Section IV of this paper.

[35] Scott Hempling, "A Letter to Governors and Legislators: On Appointing Excellent Regulators," (November 2010), available at http://www.nrri2.org/index.php?option=com_content&task=view&id=295&Itemid=38

consumers to modify that use. This task is further complicated because smart grid development is just beginning, expanding the list of variables as parties learn more.

The key conflicts among the multiple interests involved in providing and using smart grid data include:

1. The conflict between the utility's appetite for customer data and the customer's concern that that data will be misused.

    - Utilities want to collect as much data as possible regarding energy usage, but the current rules for storing and protecting that information may prove insufficient.
    - Customers want to provide input on decisions regarding when and how their data will be used, how long it will be stored, and who will ensure its accuracy.

2. The conflict between the utility's interest in using customer data to develop its own proprietary products and adopting open standards for competitive product development.

    - Smart grid data has commercial value to the utility, to the consumer, and to third parties.
    - How will the monetary benefits of product development or sales of consumption data be allocated?
    - Who will determine the benefit allocation scheme?
    - Where smart grid implementation reduces utility costs, who will receive the benefits of those cost reductions, the utility or the consumer?
    - How do we prevent the utility from leveraging its unique position into an unfair competitive advantage?

3. The conflict between commercial interests and consumer privacy.

    - Third-party developers (and utilities to the extent they seek to play an entrepreneurial role) want consumer data to develop new products and services and to identify new ways to sell old products.
      Consumers want to control whether their data will be shared at all and, if so, with whom and with what conditions.

4. The conflict between society's interests and consumer privacy.

    - Individual energy consumption data is necessary to develop incentives for reducing energy use.
    - Consumers may not want others to see or evaluate their individual energy usage patterns.

Regulators should focus on three principles in resolving these conflicts as they begin to determine who should control the release and use of smart grid data.

First, decisions regarding the control and use of personal energy consumption data depend on the ultimate use for that data. If consumer consumption data will be used for a public interest purpose, for example, deciding whether new generating facilities are required, the decision rests with the commission. If the purpose is commercial, for example developing software to help customers evaluate energy usage, the decision belongs to the customer.

Second, as **a default, utilities may use individual consumption data only for commission-defined public interest purposes (i.e., to carry out their obligation to serve, such as for grid operations). With customer consent, utilities may use individual consumption data for entrepreneurial purposes, such as to provide new products and services, but before doing so must demonstrate to the commission that they do not have an unearned competitive advantage over other providers.** That is, the utility should not have a right of access to consumer consumption data greater than the utility's competitors. Once a customer has agreed to the sharing of data with others, it must be provided equally to competing companies (including utility affiliates, software companies, and other third party vendors). Utilities must inform consumers and the commission of the intended uses for the data they collect. Public interest purposes for consumer data include initiating and billing for service, collecting outage data, dispatching repair personnel, automating processes that require consumer data but are traditionally handled manually, and other grid operations. Competitive purposes include developing products to manage usage and promoting the sale of more efficient appliances.

Third, only the consumer can decide whether and when to allow the use of her personal consumption data for commercial purposes. Consumer data beyond that used to initiate, bill, and provide electric service belongs to the consumer. It is up to the consumer and the entity that wants to use the data for a commercial purpose to negotiate the terms of that use.

The following table illustrates how regulators can use these principles to determine when regulation is necessary and when commercial solutions provide a more viable method of evaluating and resolving the conflicts between the uses for smart grid data and consumer privacy concerns.

Competing Interests Require Multiple Solutions

Smart Grid Capability/Benefit	Value to Utility	Value to Society	Value to Consumer	Consumer Privacy Concern	Mitigation Strategy	Who Regulates?
Remote reading and billing of usage; improved performance; automated outage notification	Reduced personnel costs; increased billing accuracy and timeliness	Reduced carbon emissions (no driving); minimize time lost to power outages	Accurate and on-time billing; no need to wait for meter reader; real-time incentive to adjust usage	Information security; risk of identity theft; incorrect or incomplete information	Network security design; consumer access to and correction of data errors	Commission
Reduced demand/improved transmission planning	Reduced costs; better service	Improved environment	Reduced costs	None	N/A	Commission
Utility and consumer load management	Reduce peak demand	Reduced need for new facilities	Real-time energy management	Intrusion into energy use patterns; utility may try to control usage	Customer education; clear statement of utility and customer responsibilities	Commission
Detailed energy use profile	New products and services; reduced demand	Reduced demand	Real-time energy management; reduced costs	Personal information may be leaked to wrongdoers	Customer must opt into profile development	Commercial agreement; commission enforcement of "bad acts"
Commercial product development	Enhanced revenue	N/A	Energy management solutions	Overzealous marketing	Consumers decide when and how to share data	Commercial contracts; commission enforcement of "bad acts"

IV. Existing Federal and State Privacy Rules Provide a Foundation for Developing a Smart Grid Data Privacy Policy.

The telecommunications industry has been addressing questions regarding consumer information privacy since Congress passed the Telecommunications Act of 1996. The FCC's Customer Proprietary Network Information (CPNI) rules address privacy questions similar to those raised by the deployment of the smart grid. The FCC classifies consumer data based on the potential for harm caused by the disclosure of personally identifiable information (for example, identity theft caused by the release of account and billing information) and provides a process for protecting that data, as well as obtaining permission to use it for specific purposes such as installing and billing service or marketing service bundles. Although the CPNI rules do not specifically address all the issues raised by the smart grid (for example, providing data to third parties to manage consumer energy consumption), they provide regulators with an example of the way in which another industry has successfully adopted a regulatory approach for protecting sensitive consumer information from unauthorized release while simultaneously allowing its use for other purposes.

Other federal agencies and the states are also addressing consumer privacy issues. The Federal Trade Commission (FTC) has developed standards for protecting consumer information and is currently reviewing the need for privacy standards to control the use of personal data gathered from internet users. Texas and the District of Columbia have energy privacy rules, and proceedings to develop rules are underway in California, Colorado Illinois, and New York.

This section reviews the FCC, FTC, and existing state rules.

A. The FCC's data protection rules address the need for telecommunications carriers to collect and share consumer data while protecting personal privacy.

The FCC rules for protecting customer information based on the risk to privacy from its misuse provide a useful starting point for developing a regulatory policy that protects consumer data from misuse or unapproved release, while still allowing that data to be used when necessary to meet the goals of the smart grid. The FCC rules identify three categories of information that must be protected: (1) customer proprietary network information (CPNI), (2) aggregate information, and (3) subscriber list information, and set different protection standards for each.

1. Customer Proprietary Network Information

The FCC 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.[36]

CPNI includes billing data, service installation data, account information, and other data that could individually identify a customer to others, including the actual telephone numbers to which a customer places calls. This information is equivalent to the specific energy event data discussed in Section II of this paper.

Because the misuse or inadvertent release of CPNI could harm customers, the FCC allows this data to be used only for specific purposes, such as billing, initiating new service, and repairing service problems. CPNI data may be provided to law enforcement after the receipt of a properly executed subpoena. [37]

Carriers who want to use CPNI data for other activities, such as marketing additional services or products to existing customers, must notify customers and seek specific permission for those uses in advance. The CPNI rules require:

> A telecommunications carrier [to] obtain customer approval to use, disclose, or permit access to CPNI to market a customer service to which the customer does not already subscribe to from that carrier. [38]

Customers must actively agree to allow their personal information to be used for marketing or other purposes. CPNI data cannot be sold or transferred to others without the customer's direct consent. [39] Customers may consent in writing, verbally (with third party verification), or via electronic means. Carriers must keep records of this consent.[40]

Most important, customer notifications about the use of CPNI data must be specific and understandable.

> Customer notification must provide sufficient information to enable the customer to make an informed decision as to whether to permit a carrier to use, disclose or permit access to, the customer's CPNI.

---

[36] *FCC-02-214, §64.2001*

[37] *FCC-02-214, §64.2006.*

[38] *FCC-02-214, §64.2007(a)*

[39] The CPNI rules provide specific exceptions for information necessary to protect life and safety (such as wireless 911 location information), bill third parties for services rendered, avoid the fraud, and provide inbound marketing, administrative, or referral services to customers who call the carrier for that help. FCC-02-214, para.7

[40] *See FCC-02-214, §64.2007(b)*

(i) The notification must state that the customer has a right, and the carrier a duty, under federal law, to protect the confidentiality of CPNI.

(ii) The notification must specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.[41]

2. Aggregate data

Companies can combine data from multiple customers to provide information regarding service usage by specific customer groups. Section 222(f)(2) of the Telecommunications Act defines aggregate customer information as "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed."[42] The FCC rules require local exchange carriers (LECs) to make aggregate customer information available to competitors on reasonable and nondiscriminatory terms and conditions.

Telecommunications companies use aggregated telecommunications data to market additional services and products to specific classes of customers. Because the data has been aggregated to avoid the potential for individual customer identification, the risk of harm from misuse is reduced. Aggregated data does not require specific customer consent for use, as long as the utility removes customer identifiable information.

Energy usage data transmitted over the smart grid could be aggregated and used in the same way as telecommunications data. For example, utilities or third party providers could aggregate energy consumption data at the sub-division or neighborhood level to determine what types of appliances are used by these customers, to propose new services, plan for electric vehicle charging stations, plan additional capacity, and so forth.

3. Subscriber list information

This category of data generally includes subscriber names, addresses, and telephone numbers. Telecommunications use this data to create telephone books and other listing services. Utilities must provide raw subscriber list information to other companies (including third parties) under non-discriminatory terms and conditions and with non-disclosure agreements that protect both the company and consumers.

Energy subscriber list information may be useful to equipment manufacturers who want to offer bulk upgrades to customer equipment or energy saving audits to users of specific types of equipment. Regulators should evaluate the benefits of requiring electric utilities that maintain this same type of information to provide it to others on a non-discriminatory basis .

---

[41] *FCC-02-214, §64.2007.2 (i) and §64.2007.2 (ii)*

[42] FCC-02-214, para.11

4. Carriers must train their personnel and protect consumer data.

Because the utility collects, stores, and transmits the customer's personal data, the FCC rules put the onus for managing the receipt and use of this data on the utility. They require the utility to educate its employees and customers on the definition of private data, the data elements of which it is comprised, and the allowed (and disallowed) uses for this data.

Companies must develop written policies for protecting customer information and train their employees about how to use and protect private customer information on a regular basis.[43] Most importantly, they must develop mechanisms for notifying customers and the FCC of the willful or accidental disclosure of proprietary information. The FCC requires carriers to notify it in writing of "any instances where [data protection] mechanisms do not work properly."[44]

5. Enforcement

The CPNI rules are enforced by the FCC. Failure to meet the CPNI rules, including failure to train employees, notify customers of the way in which their data will be protected, or the release of data without customer permission is punishable by fines.

B. The FTC Fair Information Practices Principles address the core requirements for protecting consumer privacy.

The FTC's Fair Information Practices Principles also provide guidance on balancing personal privacy with the need for consumer data.[45] Although these principles are voluntary, they address many of the concerns about the privacy of smart grid data voiced by consumers.

The FTC proposes five core principles that companies should observe to protect consumer privacy: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

First, companies who collect consumer data must notify consumers in advance of the purpose for requesting data. Consumers should be provided with information on the way in which the data collector will ensure the confidentiality, integrity and quality of the data. Consumers should have the opportunity to review that data periodically and contest its accuracy in the same way that they can review and clarify credit rating data.

Second, companies collecting consumer data should provide options for collecting and using that data. As we have noted previously, energy consumption data is required to install,

---

[43] See *FCC-02-214, §64.2009(a),* Telecommunications carriers must train their personnel as to when they are, and are not, authorized to use CPNI, and carriers must have an express disciplinary process in place.

[44] *FCC-02-214, §64-2009(f).*

[45] Federal Trade Commission, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm

bill, and maintain utility service, but the Fair information Practices principles go beyond this requirement to recommend that companies give consumers the opportunity to consent to f other uses for consumption data, product sales or promotions or the transfer of data to third parties.

Third, consumers should be able to access the information companies collect about them and to contest its accuracy and completeness.

Fourth, companies should make sure the data they collect is accurate and secure. This includes taking actions to prevent loss, data corruption, and misuse. Companies that collect consumer data should audit their privacy policies and procedures on a regular basis to ensure that they are working as designed.

Fifth, privacy rules must be enforced and consumers must be provided with an opportunity for redress. As the FTC points out, without enforcement "a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles."[46] Enforcement can range from industry self-regulation to the federal remedies established by the FCC in their proprietary information access standards.

The FTC has recently begun to evaluate the need for creating rules to protect consumers who provide data about their location or other information while surfing the internet. A December 2010 staff report proposes that the FTC create

> a framework [for internet security] to balance the privacy interests of consumers with innovation that relies on consumer information to develop beneficial new products and services. The . . . report also suggests implementation of a "Do Not Track" mechanism – likely a persistent setting on consumers' browsers – so consumers can choose whether to allow the collection of data regarding their online searching and browsing activities.[47]

The FTC recommends that consumers be able to opt out of information gathering and use and may require companies that use consumer information gained from internet browsing to provide standardized notices of their information use and security policy. Like the FCC, the FTC recommends that companies "undertake a broad effort to educate consumers about commercial data practices and the choices available to them."[48]

---

[46] Federal Trade Commission, Fair Information Practice Principles, p 2

[47] FTC Staff Issues Privacy Report Offers Framework for Consumers, Businesses, and Policymakers, FTC Privacy Press Release, 12/2/2010, available at http://ftc.gov/opa/2010/12/privacyreport.shtm

[48] FTC Staff Issues Privacy Report Offers Framework for Consumers, Businesses, and Policymakers, FTC Privacy Press Release, 12/2/2010, available at http://ftc.gov/opa/2010/12/privacyreport.shtm

C. Rules for smart grid privacy are in place or under review in a number of states.

Concerns about privacy must be addressed on the state level, as no single agency (for example, FERC, DOE, or the FTC) has jurisdiction to specify federal rules to protect retail consumer energy usage data. A cohesive approach to consumer protection on this issue will harmonize consumer expectations, set uniform expectations for the various electric utilities operating across state borders and foster well-settled law in the area.

As privacy law evolves to catch up with smart grid and smart meter technology, several states are in the vanguard. For example, Texas and the District of Columbia already have rules regarding the privacy of energy data in place.

Texas bases its rules for smart grid privacy on the telecommunications privacy standards discussed in Section IV.B above. The Texas regulations require electric utilities to protect private customer information and seek customer approval for disclosure.[49]

Like the FCC rules, §25.272(c) of the Texas rules define customer proprietary information as:

> Any information compiled by an electric utility on a customer in the normal course of providing electric service that makes possible the identification of any individual customer by matching such information with the customer's name, address, account number, type or classification of service, historical electricity usage, expected patterns of use, types of facilities used in providing service, individual contract terms and conditions, price, current charges, billing records, or any other information that the customer has expressly requested not be disclosed [50]

The Texas rules require customer consent to release customer specific information:

> Except as specified in subsection (a) of this section, a REP or aggregator shall not release proprietary customer information, as defined in §25.272(c)(5) of this title (relating to Code of Conduct for Electric Utilities and Their Affiliates), to any other person, including an affiliate of the REP, without obtaining the customer's verifiable authorization.[51]

---

[49] The Texas PUC has used the FCC CPNI rules as the foundation for its smart grid regulations. See http://www.puc.state.tx.us/rules/subrules/electric/25.272/25.272.pdf.

[50] PUCT Rule §25.272(c), see http://www.puc.state.tx.us/rules/subrules/electric/25.272/25.272.pdf

[51] PUCT Rule §25.472(b); §25.474(c) provides the standards for releasing this information.

The Texas rules allow utilities to provide mass listings of customer data (including name, billing address, rate classification, monthly usage for the most recent 12-month period, meter type, and account number or electric service identifier) to other companies to allow competitive bidding for specific programs without requiring customer approval in advance, but must notify customers in writing of this practice to allow them to opt-out.

The District of Columbia also provides specific rules governing how electric utilities must protect customer information. Section 34.1507 of the Public Utility Code covers the sharing of customer specific energy data:

> (a)(1) Unless a customer consents in writing, a market participant or the electric company may not disclose information that: (A) Is about the customer; and (B) Was supplied to the market participant or electric company by the customer.
>
> (b)(1) Unless a customer consents in writing, a market participant or the electric company may not use information of the type specified in subsection (a)(1) of this section for any purpose other than the purpose for which the information was originally acquired.

The utility commissions of California, Colorado, Illinois, and New York have open proceedings to develop privacy rules for energy data. Generally, the participants in each of the open proceedings have recommended that commissions adopt rules similar to those used in the telecommunications industry.[52] In a report written for the state smart grid task force created by SB 10-180, Colorado suggests two additions: (1) notice to the customer of the purpose for collecting the customer-specific information and (2) a requirement that the information be accurate.[53] The New York Smart Grid Consortium Road Map recommends further study to ensure ubiquitous protection for customer proprietary information.[54]

In California, the Center for Democracy and Technology and the Electronic Frontier Foundation jointly recommended that the CPUC adopt privacy protections based on the FTC's Fair Information Practice principles. The California proposal includes a requirement that utilities specify the purpose of the information they collect and explain how they will ensure and monitor data quality and integrity. Specifically, the recommendation includes eight principles: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Data Security, and Accountability and Auditing.[55]

---

[52] *See*, e.g., Illinois Statewide Smart Grid Collaborative: Collaborative Report, September 30, 2010, pp 20-21.

[53] Kevin Doran, Frank Barnes, Puneet Pasrich, Smart Grid Deployment in Colorado: Challenges and Opportunities, University of Colorado at Boulder, June, 2010, pp. 3-5.

[54] Smart Grid Roadmap for the State of New York, New York Smart Grid Consortium, September 15, 2010, p. 42.

[55] *Calif. Public Utility Commission Docket 08-12-009, Opening Response, filed by Center for Democracy & Technology and Electronic Frontier Foundation, in Rulemaking to Consider*

V. Recommendations for Reconciling the Multiple Interests in the Smart Grid Privacy Debate

The task for regulators in the smart grid privacy debate is to select a decision path that reconciles the interests of the disparate players—utilities, consumers, and third-party product developers and marketers—with the need to use consumer energy data to attain the environmental and social benefits of the smart grid. To do this, regulators will need to answer the three key questions we posed at the beginning of this paper.

1. Is all personal data the same, or should it be placed into categories that require different privacy treatment?

2. By what method should consumers consent to the use of their data by the utility, its affiliates, and other parties? Should the regulator assume consent simply because consumers agree to participate in smart grid programs or is proactive consent required? Should the requirements for consent vary depending on the type of data that will be shared?

3. Who will receive any monetary rewards generated by the sale of consumer energy data?

The following paragraphs provide a construct for understanding and embarking on this journey.

A. There is no single answer to the question of smart grid privacy; the components of the solution depend on intent and need.

Privacy is about intent, expectation, and behavior. The key to achieving the benefits of the smart grid while respecting user privacy is addressing privacy concerns in advance, before the utility brings the commission a request to build a smart grid, implement smart metering, or offer customers a smart pricing plan. These privacy solutions must be crafted so that they apply to all players—the utility, its regulated and non-regulated affiliates, its suppliers, and the third parties that will develop products for collecting and managing energy use based on smart grid data.

There are four main components to the solution:

1. Define the information utilities will collect, determining with whom and for what purposes it will be shared, and assessing the need for protecting that data. By categorizing the data that will be collected and the purposes for which it will be used, regulators can identify its potential to benefit or harm consumers, and determine whether rules are needed. NIST refers to this process as a Privacy Impact Assessment (PIA).

Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's Own Rulemaking Motion to Actively Guide Policy in California's Development of a Smart Grid System, October 15, 2010, p. 5.

> A PIA is a comprehensive process for determining the privacy, confidentiality, and security risks associated with the collection, use, and disclosure of personal information. PIAs also define the measures that may be used to mitigate and, wherever possible, eliminate the identified risks.[56]

2. Ensure that customers understand what data will be shared and under what terms and conditions. As explained in Part II of this paper, the key customer concern regarding smart grid data collection is the creation of an energy profile that could impact their personal or financial safety.[57] Education and communications are key to addressing this concern. As the Maryland Public Service Commission's order on Baltimore Gas and Electric's (BG&E) Smart Meter tariff makes clear,

> the success of this [smart metering] Initiative, and the likelihood that customers will actually see the benefits this project promises, depend centrally on the success of the Company's customer education and communication effort.[58]

But education does not consist simply of notifying customers of the data elements that utilities may use and share; it also includes developing a policy for allowing customers to agree to sharing information beyond that required to bill and install service with others. All vendors, including a utility's non-regulated affiliates, that will use customer data to develop products, manage consumption, or market services to consumers based on energy consumption data must include a description of their privacy policies in their customer offers. Commissions should work with the relevant state agencies and federal entities such as the Federal Trade Commission to ensure that privacy is considered from the beginning to the end of the supply chain.

3. Require utilities to implement internal privacy training programs and internal audits of privacy processes and procedures. Utilities will not meet customer privacy requirements unless their employees understand the rules and follow them. All employees with access to consumer data should be trained on privacy requirements on a yearly basis. Utilities should certify that this training has taken place on a yearly basis.[59]

4. Enforce and revise. There will be violators; and not all rules will work well. These violations and rule failures must be reported and processes amended to correct errors. State

---

[56] *National Institute of Standards and Technology Interagency Report 7628,* vol. 2, pg15

[57] See http://www.realtime-itcompliance.com/privacy_and_compliance/2009/09/10_smart_grid_consumertoutilit.htm for a discussion of consumer's top 10 energy privacy concerns.

[58] *Maryland Public Service Commission, Order No. 83531 8/13/10),* p 43 and *Order No. 83410 (6/21/10).*

[59] Although self-certification has been successful in implementing other standards certification programs such as the Sarbanes-Oxley Act, regulators should monitor utility compliance and reserve the power to ensure compliance in other ways, including developing sampling or testing programs.

commissions and legislatures should work together to develop a system for enforcing both failures to implement the data privacy requirements and breaches of security. These requirements should include customer notice procedures, as well as fines if applicable. 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.

B. Should rules be state-specific or could national or regional collaboration lead to a stronger conclusion?

The smart grid is not a single entity that will impact consumers in a single state. As the DOE points out, in the long term, the smart grid will become a national network of intelligent generation, transmission, and distribution facilities. Because similar issues regarding privacy standards will be faced wherever the smart grid is implemented, regulators must consider whether it is better to regulate each application individually or set a smart grid privacy policy at the national or regional level, with equivalent rules applied to all participants,.

Individual state rules can be crafted rapidly, but these rules will not necessarily be uniform or consistent. National or regional rules will provide uniformity, but the time required to implement such rules may unnecessarily delay smart grid development or cause further privacy concerns. We discuss the pros and cons of these options so that regulators may examine them in determining how to develop a smart grid privacy policy.

1. Create a national or regional smart grid privacy policy

Pro:

- A national policy will be consistent and uniform. Consumers will be able to understand the "rules of the road" regardless of where they live or where their energy usage takes place.
- Multi-state energy providers and third party marketers will be able to develop a single data protection policy that applies everywhere they operate.
- Enforcement policies and remedies will be the same in all jurisdictions, ensuring that like offenses are dealt with similarly.

Con:

- Creating a national policy will be a lengthy process.
- No single agency has oversight over smart grid privacy policy.

2. Create smart grid privacy policy at the state level

Pro:

- State commissions have experience in utility regulation and data privacy issues.
- Existing state rules address data privacy.
- State rules can be developed rapidly.
- Individual states have individual requirements and so need individual rules.

Con:

- State rules will not be consistent or uniform.
- Companies will be required to implement different privacy standards in each state in which they do business.
- Regional energy markets require regional solutions.

Because many state regulators are faced with immediate requests to approve the components of the smart grid in their individual states, the roadmap provided in this paper provides guidance in creating plans that could be subsumed into a national plan should one be developed. In the interim, state regulators may also work across regional lines to create similar plans for neighboring states. This process has been used successfully in the telecommunications industry where a single supplier provides service in multiple states.

C. Do consumer contracts for smart grid data require commercial or regulatory enforcement?

As the smart grid grows, equipment manufacturers, software developers, and marketers will develop new uses for the specific consumer consumption data users generate. These uses may create new "energy data" markets for consumers who want to sell or trade their individual consumption information for goods and services. As we noted previously, transaction data generated on the consumer side of the electric meter—within the consumer's premises and regarding specific consumer appliance use—belongs to the consumer. Consumers should receive any monetary benefits from their own usage data. As these markets grow, regulators will need to evaluate whether specific energy data contract requirements are necessary or whether commercial contracting rules are sufficient to protect unsophisticated consumers who are used to depending on regulation.

Regulators must address four key points in dealing with this new market: (1) whether they should create standard contracts for consumer energy data, (2) whether third party energy management companies should be regulated or certificated at the state level, (3) what recourse consumers will have should their private data be misused, and (4) who should adjudicate disputes regarding these contracts?

VI. Conclusion

The smart grid brings utilities, consumers, and society a range of benefits and risks. It will help utilities reduce costs, better manage assets, and minimize the frequency and duration of outages. It will allow customers to lower their electric bills by planning their consumption in "real time," moving discretionary energy-intensive activities to off-peak periods and modifying or even eliminating the use of inefficient appliances to reduce costs and protect the environment. It will benefit society by improving the operation of the national energy grid, lowering emissions from fossil fuel generation, and encouraging the use of renewables. But with these benefits comes the challenge of balancing the risks caused by the potential mishandling of the new, highly-granular consumer energy consumption data against the rewards of a robust smart grid.

In this paper, we have considered definitions of the smart grid, examined the benefits and risks of sharing energy usage data, and provided examples of privacy protection rules from the telecommunications industry, the FTC, and the states that could serve as the foundation for developing state, regional, and national smart grid privacy policy. We have also provided principles for guiding commission decision-making and recommendations for resolving the tension between the multiple parties in the smart grid privacy debate, and explored the question of who should develop smart grid policy—the states or national bodies such as Congress, the DOE, or FERC. Finally, we proposed four key components for developing a smart grid privacy policy maximizes the benefits of the smart grid while protecting consumer privacy.

The Components of Smart Grid Policy Depend on Intent and Need

1. Define the information utilities will collect: • **With whom will it be shared?** • **For what purpose?** • **What protection will be required?**
2. Ensure that customers understand: • What data will be shared? • Under what terms and conditions?
3. Require privacy training programs: • Train utility employees yearly. • Require certification • Audit compliance
4. Enforce and revise: • Report privacy breaches • Amend processes to correct errors • Review and evaluate

The smart grid privacy debate is just beginning, giving regulators a unique opportunity to forge a workable regulatory solution to the privacy issues involved in developing the infrastructure of the smart grid.