Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Smart Grid Technology	)	GN Docket Nos. 09-47, 09-51, 09-137
	)	
DA 09-2017	)	

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

Jennifer M. Urban
Elizabeth Eraker
Longhao Wang

Samuelson Law, Technology & Public Policy Clinic
UC Berkeley School of Law
585 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7338

on behalf of:
Center for Democracy & Technology

October 2, 2009

Table of Contents

Summary……1

I. Introduction……2

II. Overview of Smart Grid Data Collection and Use……3

a. Data Collection by Utilities……4

b. Data Sharing and Data Collection by Third Parties……6

c. Data Storage……7

d. Data Usage……8

III. Consumer Privacy and Security Implications of Smart Grid Data Collection and Sharing……9

IV. Legal and Policy Considerations……12

a. Inadequacy of Current Privacy Rules……12

b. Key Privacy and Security Considerations in Developing Smart Grid Rules……14

c. Key Privacy and Security Considerations in Developing Smart Grid Technologies……16

V. Conclusion……17

Summary

In considering the implications of Smart Grid technology as part of its development of the National Broadband Plan, the Commission should carefully consider, and address in its actions, the privacy and security issues that will emerge from the widespread implementation of this technology. These new technologies will collect an unprecedented amount of highly detailed information about consumer energy consumption. This granular usage data reveals deeply personal information about consumer habits, and about consumer activities within the private space of the home. Given both the sensitive nature and high commercial value of this data, utilities and third-party businesses will be eager to make use of it, as will law enforcement investigators and, unfortunately, criminals. As such, a lack of care around this data will pose serious privacy and security risks for consumers. These issues are further complicated by the reality that the Smart Grid, at present, is governed by a patchwork of state and federal laws. Neither in isolation nor taken together do these existing laws provide adequate protection for the categories and quantities of data that may be generated by the Smart Grid.

Realizing the likely benefits of the Smart Grid, including improving energy efficiency, reducing utility bills, and protecting the environment, will require consumers to trust that these new technologies will be protective of personal information and secure against threats. At a minimum, any rules governing the development of Smart Grid technologies should require:

- Transparent notice to the consumer of data collection practices;
- Minimized data collection, access, and retention;
- Meaningful choice for consumers regarding the use and disclosure of their usage information;
- Reasonable consumer access to, and the ability to correct or dispute, all usage information held by utilities or third-party providers; and
- Meaningful security controls to protect consumer usage data, along with adequate remedies for unauthorized use.

In addition to legal and procedural protections, the Commission should ensure that privacy is integrated at every point in the network via appropriate technological design at the outset, so that privacy and security do not have to be later retrofitted onto the system. Two key design principles the Commission should consider are:

- Designing the Smart Grid communications network to ensure the privacy of data transmissions along the entire communications path and at all points of storage; and
- Designing SmartGrid technologies to minimize the amount of consumer data that leaves the house to only such information as is actually required for demand response benefits to be realized.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Smart Grid Technology	)	GN Docket Nos. 09-47, 09-51, 09-137
	)	
DA 09-2017	)	

The Center for Democracy & Technology ("CDT") respectfully submits these comments in response to the Commission's Public Notice, DA 09-2017, regarding the implementation of Smart Grid technology. CDT is a nonprofit, public interest organization dedicated to preserving and promoting openness, innovation and freedom on the decentralized Internet**.**

I. Introduction

In modernizing the electrical grid to provide both consumers and utilities with the ability to monitor, control, and predict energy use, Smart Grid technology holds great promise. The technology also implicates important consumer privacy and security issues that warrant attention as we develop the technical and regulatory infrastructure underlying the new grid.

New funding allocated under the American Recovery and Reinvestment Act of 2009 ("ARRA") is likely to rapidly accelerate the implementation timeline, connecting most U.S. households to the Smart Grid in the next decade.[1] The benefits of this transition are expected to include: fostering more efficient energy use, reducing greenhouse gases, enhancing grid defenses against attack and outage, and lowering consumers' energy bills. To realize these benefits, the U.S. must make a profound change in the underlying design of our electrical infrastructure, transitioning from a relatively isolated grid operated by a small set of highly trained experts to a completely-connected, less-bordered broadband network that invites widespread participation from individual consumers and their appliances.[2] At the core of the new grid's functionality, as envisioned by many proponents, is the collection and use of fine-grained data about consumer energy use. In order to enable more efficient energy decisions, it is assumed, the Smart Grid depends on the use of much more detailed information about load balance

[1] This is an extrapolation from the Federal Energy Regulatory Commission (FERC) estimate that 40 million homes and business will have smart meters deployed by 2010. *See* FERC, *Assessment of Demand Response and Advanced Metering 2007*, Sept. 2007.
[2] *A Voice for Smart-Grid Security*, Fortnightly, 147 No. 7 Pub. Util. Fort. 24, July 1, 2009.

and energy use than is presently collected.[3] Many Smart Grid proposals rely on the ubiquitous collection of information about consumers' activities within the home, a space traditionally protected by a strong privacy interest. As the Commission considers the implementation of Smart Grid technology, and utilities and technologists proceed with planning and deployment activities, the time is ripe to address the important privacy and security issues associated with the Smart Grid concept.

Ensuring that the Smart Grid incorporates significant protections for consumer privacy is essential to achieving widespread acceptance and adoption of this exciting new technology. Privacy is an essential building block of trust in the digital age. In the context of a digitized electrical grid, consumers must be assured that the data about their energy usage is kept confidential and secure, or privacy concerns may undermine use of the modernized grid. Building privacy and security protections into the technology now will be less expensive than attempting to address these issues in the future, and will make the grid more adaptable to changing threats to privacy and security as use increases.

We thank the Commission for seeking comments on the implications of Smart Grid technology at this relatively early point in its development, and especially for raising consumer privacy and security issues in the inquiry.[4] Building on our submission in the National Broadband Plan proceeding,[5] these Comments aim to highlight the importance of protecting consumer privacy and implementing critical security protocols. We recommend several principles protective of those interests for the Commission's consideration as it evaluates new infrastructure and technologies for the Smart Grid in developing a broadband plan that advances "energy independence and efficiency."[6]

II. Overview of Smart Grid Data Collection and Use

Smart Grid technologies have the ability to collect far more detailed information about consumers than previous systems.

This enhanced access to consumption information promises several benefits: it allows consumers to track their energy use at different times of the day, and enables utilities to implement time-of-use pricing, whereby consumer are charged higher prices for energy during peak demand periods and charged less when energy demand is low. In response, consumers can defer their energy consumption from peak demand periods to a

---

[3] Patrick McDaniel and Stephen McLaughlin, *Security and Privacy Challenges in the Smart Grid*, IEEE, May/June 2009.
[4] *See, e.g.,* Question 4(c).
[5] Center for Democracy & Technology, *In the Matter of A National Broadband Plan for Our Future*, GN Docket No. 09-51, available at http://www.cdt.org/speech/20090608_broadband_comments.pdf.
[6] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 600(k)(2)(D), 123 Stat. 115 (2009).

later hour. This "demand-response" process improves energy efficiency by reducing peak demand, and at the same time, reduces consumer's energy bills and better protects the environment. [7]

In this section, we briefly review examples of collection, sharing, usage and storage of data about consumers by utilities and third parties, each of which raise potential concerns that could be mitigated by taking a proactive approach.

a. Data Collection by Utilities

With the advent of the Smart Grid, utilities will likely collect far more information about consumers than in the past. Traditionally, analog meters are read once a month or even less by the utilities; at each reading, utilities record consumers' aggregate usage since the last reading for billing purposes.[8] With smart meters, utilities are able to monitor meter readings in real-time[9] or at small time intervals.[10] The information about in-home activities that can be determined from this data is radically different from the traditional model, because variations in consumption patterns can reveal detailed personal habits and the use of specific home appliances.[11]

In addition to gathering meter readings at a much finer level of specificity than traditional analog meters, Smart Grid technologies will enable utilities to collect new types of information. For example, in PG&E's SmartAC program, the utility company installs programmable thermostats for consumers' air conditioners, which communicate with the utility company.[12] A utility company might use the communication channel to display messages on the screen of the thermostat such as weather warnings, greetings,

---

[7] Department of Energy Electricity Advisory Committee, *Smart Grid: Enabler of the New Energy Economy*, http://www.oe.energy.gov/DocumentsandMedia/final-smart-grid-report.pdf, at 9.

[8] Jack I. Lerner and Deirdre K. Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 Stan. Tech. L. Rev. 3.

[9] *See* Itron News, *Itron Takes Commanding Role in Real-Time Energy Monitoring by Partnering with Google and Microsoft*, http://news.itron.com/Pages/ami02_0709.aspx.

[10] Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies,* May 9, 2009, available at SSRN: http://ssrn.com/abstract=1462285.

[11] Jack I. Lerner and Deirdre K. Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 Stan. Tech. L. Rev. 3.

[12] PG&E, *SmartAC Frequently Asked Questions: What are the SmartAC technology options?,* http://www.pge.com/myhome/saveenergymoney/energysavingprograms/smartac/faq/.

and system maintenance notices.[13] Consumers could also configure their thermostats on the utility company's website,[14] giving the utility company information about consumers' temperature preference in their homes. It is possible that utility companies could use the same communication channel to collect real-time readings on the temperature of consumers' homes, which, if temperature is an indicator of presence, might reveal that residents are not home (e.g., a thermostat is left at 55 degrees in the winter for several days).

If consumers choose to register their smart appliances or home area networks (HAN) with the utility company in order to enroll in utility-sponsored programs, detailed information about their appliances or HAN could also be collected by the utilities.[15] For example, in the use case describing Southern California Edison's SmartConnect program, consumers are asked to provide identification information about their account and smart appliances in order to register those devices with the utility.[16] A similar approach has been adopted in the OpenHAN standard, which is a part of the National Institute of Standards and Technology's (NIST) project to develop interoperability standards, the Smart Grid Interoperability Standards Framework.[17] Under the OpenHAN standard, consumers need to provide "unique registration information from the HAN Device (e.g. registration key, serial number)" for device-to-utility registration.[18] The exact nature and content of information collected about smart appliances is unclear at this time, and what is collected will likely continue to evolve. It is entirely possible that collected information about smart appliances could include brand, date of manufacture and model, which could reveal highly personal information, such as consumers' income level and purchasing preferences. NIST is considering the issue of appliance data collection, which will likely influence the approaches adopted by many utilities. Responses to the Notice's Questions Four and Five will be helpful in informing that review, and the Commission should continue to seek information about what data is being collected as the technology develops.

---

[13] PG&E, *Honeywell Thermostat Operating Manual*, http://www.pge.com/includes/docs/pdfs/shared/smartac/thermostatuserguide.pdf.
[14] PG&E, *SmartAC Thermostat Programming Website Guide,* http://www.pge.com/includes/docs/pdfs/shared/smartac/pg-wc-7e_webguide_tstat[f]-screen.pdf.
[15] UtilityAMI Working Group, *UtilityAMI Home Area Network System Requirements Specification*, Aug. 2008.
[16] Southern California Edison, *SmartConnect Use Cases C5*, http://www.sce.com/NR/rdonlyres/EC46A2AC-9D43-4674-90A7-CBE47F362CDE/0/C5_Use_Case_090105.pdf.
[17] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0,* Sept. 2009, http://www.nist.gov/public_affairs/releases/smartgrid_interoperability.pdf, at 34.
[18] UtilityAMI Working Group, *UtilityAMI Home Area Network System Requirements Specification*, Aug. 2008, at 71.

b. Data Sharing and Data Collection by Third Parties

Since the Smart Grid heavily relies on information technology, the utilities may make use of third-party telecommunication networks[19] or web portals[20] to offer and enhance their services. Under these arrangements, the information collected by the utilities, such as the detailed consumption information described above, could be shared with third parties.

Consumers' choices about this sharing of their information with third parties may be limited. For instance, utilities may make use of third-party wireless networks to communicate with smart meters and other Smart Grid devices. Depending on how these services are structured, they may or may not fit within existing regulatory frameworks intended to protect the privacy of communications and, depending in part on how terms of service are defined, consumers may end up sharing their data with third-party wireless vendors. On the other hand, utilities may allow consumers to choose whether to make use of certain services, such as third-party web portals, to manage their utility usage data. As such, choices may evolve allowing users to pick among a range of third-party providers with which they would prefer to share utility usage data.[21]

In addition, direct-to-consumer third-party service providers are likely to collect various types of information. For example, in order to provide recommendations to consumers about how to conserve energy, Microsoft Hohm encourages consumers to provide not only meter reading data, but also detailed information about the physical conditions of their homes, such as the number of windows and doors, the location of the home, its year of construction, and its type of heating system. Google Power Meter collects smart meter reading data from utilities and offers consumers a web interface allowing them to visualize their data through a graphical display. As discussed further below, consumers should have control over how their personal usage data is collected, used and stored by direct-to-consumer services. We discuss third-party providers' interest in Smart Grid information in Section III, below.

---

[19] PG&E, *SmartMeter—How the System Works*, http://www.pge.com/myhome/customerservice/meter/smartmeter/howsystemworks/ (describing how "the access point device aggregates, encrypts, and sends the data back to PG&E over a commercial third-party network").

[20] *See* utility partners of Google PowerMeter listed at http://www.google.org/powermeter/partners.html, and utility partners of Microsoft Hohm, listed athttp://mshohm.orcsweb.com/partners/.

[21] San Diego Gas and Electric, *Monitor your home electricity use from the web*, http://www.sdge.com/myaccount/energynetwork/ (stating that "SDGE is developing a new online platform that will provide smart meter customers with a list of choices, including Google PowerMeter…[w]ith this platform, in the future, customers can decide where and how they receive their energy use information").

Finally, and perhaps most importantly, utilities and others collecting data as part of the Smart Grid are going to face substantial economic incentives to sell such data to third-party aggregators. Given the fine granularity and great variety of information collection enabled by these technologies, information services companies may be eager to use Smart Grid data to enhance existing portfolios of personal information about consumers to be useful to businesses exploiting such profiles to offer their products and services. As part of the Commission's proceeding, it should investigate any contractual or other relationships between utilities and entities looking to purchase or gain access to the energy consumption data held by utilities, in order to strengthen consumers' understanding of current and future sharing practices and to develop suitable privacy protections.

c. Data Storage

Currently, utilities store many years' worth of customers' meter reading data to facilitate customer dispute resolution, as well as load and other research. Assuming that these data retention practices persist with the implementation of Smart Grid technologies, utilities will be storing much larger amounts of consumer data for a considerable length of time. Instead of one meter reading or less per month for each consumer, smart meters enable utilities to collect significantly more information about consumers' actual energy use over a long period of time, leading to the retention of a potentially far more revealing body of information about consumers' daily lives. Practically speaking, this means that a customer's monthly record of energy usage might expand from one data point to 750 to 3,000 distinct and time-stamped points reflecting actual energy usage.[22]

A consumer's meter reading data may also be stored by third-party companies offering Smart Grid-based products and services to consumers. For instance, Microsoft Hohm, the consumer web portal tracking energy use, states in its Terms of Use that if a user deletes his or her account, Microsoft "will not retain" any of the user's data, implying that information will not be stored if the account is deleted.[23] The similar Google PowerMeter states in its FAQs that "[a]ll energy data received by Google PowerMeter will be stored securely, and users will be able to delete their energy data or ask their utility to stop sending data to Google PowerMeter at any time."[24]

Far more information is needed about the retention and security policies governing data stored by utilities and third-party service providers, including the exact

---

[22] Jack I. Lerner and Deirdre K. Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 Stan. Tech. L. Rev. 3.

[23] Microsoft, *Hohm Terms of Use*, http://www.microsoft-hohm.com/Info/TermsOfUse.aspx.

[24] Google, *PowerMeter Frequently Asked Questions (FAQs)*, http://www.google.org/powermeter/faqs.html.

period of time that consumer data is stored, what protections are in place to prevent unauthorized access by data thieves or others, whether consumer information is segregated or commingled with other types of data, what procedures are in place to manage subpoenas and other requests for information, and under what, if any, circumstances data may be transferred or sold to data brokers, advertisers and other third parties. Determining the answer to these data storage questions is important because of the sensitivity and personal nature of much of the collected data, along with the risks of security breaches, and the obvious interest that companies, law enforcement officers and others will have in it, as we further explain in Section III.

d. Data Usage

Consumers' meter data is used in different ways by various Smart Grid participants. Utilities use the data for billing and load research. Third-party providers such as Microsoft Hohm use the data to display targeted advertising to consumers, as well as to recommend ways to reduce consumers' use of energy.[25] Consumers can use their own usage data to be better informed about their energy consumption and to take actions to reduce energy consumption or shift consumption to off-peak periods.[26] Law enforcement and data brokers may seek access to consumers' meter reading data to glean details of consumers' lives. The data may also be sought in the context of civil litigation, such as a divorce proceeding or custody dispute, in which energy usage data could be helpful in establishing physical presence, such as the time of day a person left the home.

As previously noted, utilities may collect information identifying consumers' smart appliances if consumers choose to register their devices with the utilities. In the use case describing Southern California Edison's ("SCE") planned SmartConnect program, SCE describes the information as being used to "ensure the specific type of Smart Appliance is available for registration in the system and confirm it meets the utility requirements."[27] The information can also be used to choose the appropriate programs the smart appliance might participate in and to authenticate the smart device.[28]

In sum, Smart Grid technologies enable the collection of highly detailed and varied data about consumers' activities, and this information is or could be collected,

---

[25] Microsoft Homn Community Blog, *Channel 10 - Podcast Microsoft Hohm*, available at http://blog.microsoft-hohm.com/news/09-06-24/Channel_10_-_Podcast_Microsoft_Hohm.aspx.

[26] NPR, *Smart Meter Saves Big Bucks For Pa. Family*, Apr. 28, 2009, http://www.npr.org/templates/story/story.php?storyId=103437607.

[27] Southern California Edison, *SmartConnect Use Cases C5*, http://www.sce.com/NR/rdonlyres/EC46A2AC-9D43-4674-90A7-CBE47F362CDE/0/C5_Use_Case_090105.pdf.

[28] UtilityAMI Working Group, UtilityAMI HAN System Requirements Specification, Aug. 2009.

stored and used by diverse entities, including utilities, third-party service providers, law enforcement, and data brokers.

III. Consumer Privacy and Security Implications of Smart Grid Data Collection and Sharing

Mapping the landscape of data uses under a Smart Grid scheme provides a helpful foundation for understanding the range of consumer issues implicated by a digital grid. While the wealth of information collected by Smart Grid technologies provides significant benefits to consumers, it also presents new privacy concerns. This unprecedented amount of information collected about consumers' energy consumption has the potential to reveal intimate details about daily lives and activities inside their homes, with serious privacy and security implications, which we explore below.

The wide-ranging privacy implications of Smart Grid data have been emphasized in the federal effort to develop standards for the Smart Grid. NIST's recently released Framework and Roadmap for Smart Grid Interoperability Standards aptly notes the privacy implications of "richer data to and from customer meters and other electric devices."[29] Specifically, NIST recognizes concerns about "the type and amount of billing and usage information flowing through the various entities of the Smart Grid, the dangers posed by data aggregation of what was considered to be 'anonymized' data, and the privacy implications of frequent meter reading that could provide a detailed time-line of activities occurring inside the home."[30]

For instance, information about home appliance use could be reconstructed from smart meter reading data by using non-intrusive appliance load monitoring (NALM) or other technologies.[31] Researchers can compile libraries of appliance load patterns and match similar patterns in the time series data of overall utility usage.[32] Some research shows that fifteen-minute interval data could pinpoint the use of most major home appliances.[33] As the interval of data collected by the Smart Grid decreases, home appliance use can be inferred from overall utility usage data with greater and greater accuracy. This gives rise to serious privacy concerns, because home appliance use reflects intimate details of people's lives and their habits and preferences. Some of the

---

[29] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0,* Sept. 2009, at 84.
[30] *Id*.
[31] Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies*, May 9, 2009, available at SSRN: http://ssrn.com/abstract=1462285, at A-1.
[32] *Id*. at 2. The construction of load pattern libraries can be manually crafted, or generated by machine learning algorithms such as a neutral network.
[33] Research suggests this can be done with accuracy rates of over 90 percent. *See* Elias Leake Quinn, *Privacy and the New Energy Infrastructure*, Feb. 15, 2009, available at SSRN: http://ssrn.com/abstract=1370731, at 28.

activities that might be revealed through energy usage include personal sleep and work habits, cooking and eating schedules, the presence of certain medical equipment and other specialized devices, and activities that signal illegal behavior.[34]

In addition, devices connected to the Smart Grid may be able to collect information above and beyond the basic usage of power—for example, the programmable thermostat described in Section II may be technologically capable of collecting temperature inside a home by using the same communication channel that the utility company uses to send messages or control signals to the thermostat. Temperature inside homes could be used to—among other things—confirm or negate the residency at an address. For instance, a very high temperature in a home on a hot summer afternoon may indicate that no one is inside the home, as would a very low temperature in the winter.

When the information collected by the Smart Grid is used for purposes unintended or unanticipated at the time of collection, privacy and security concerns are exacerbated. [35] Much of the information collected by the Smart Grid about consumers is commercially valuable, and could be resold for a profit. For instance, as the analysis of meter reading data collected by the Smart Grid reveals consumers' home activities and daily routines, the information would be commercially valuable to life insurance companies looking to adjust rates for customers with unhealthy lifestyles. Financial institutions making home mortgage loans might also be interested in the energy bills of the houses of their customers to verify whether the customers are actually living in those houses. Advertising companies offering behavioral targeting products might attempt to enhance existing consumer profiles with energy usage data revealing consumer activities and habits, following a recent trend in the merging of online and offline data sources to support more targeted third-party advertising.[36] Furthermore, smart appliance information collected by utilities when consumers register their smart appliance may reveal consumers' purchasing preferences and income level, which is valuable for the market research and marketing efforts of smart appliances manufacturers. As we noted above, data brokers, advertisers, marketing research firms, and others might also find this type of detailed information about consumer habits attractive.

The existence of Smart Grid data raises security concerns in several contexts. Criminals may seek access to smart meter reading data or other information collected by

---

[34] Jack I. Lerner and Deirdre K. Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 Stan. Tech. L. Rev. 3.

[35] For a list of other possible uses of utility usage data, *see* Elias Leake Quinn, *Privacy and the New Energy Infrastructure*, Feb. 15, 2009, available at SSRN: http://ssrn.com/abstract=1370731, at 23.

[36] For more about recent trends in data aggregation and the development of enhanced consumer profiles for advertising purposes, *see CDT's Guide to Behavioral Advertising*, http://cdt.org/privacy/targeting/.

the Smart Grid, and use this data to infer whether anybody is present in a house and to determine the most desirable time to commit a crime. In addition, because the Smart Grid enables the accumulation of personally identifiable information over long periods of time, the information could reveal behavior patterns that will likely be repeated in the future, allowing criminals to plan for future attacks. If the personally-identifying information accumulated by the Smart Grid is accessible to computer hackers or to "war drivers" monitoring a wireless network, the information could also be used by criminals to commit identity theft. For instance, many businesses and others traditionally use energy consumption data to authenticate customers, making the information particularly valuable to those attempting to stealing identities.[37] The threat to security of consumer data is exacerbated if the data transmission in the Smart Grid is not encrypted, in which case criminals may be able to easily intercept Smart Grid transmissions and acquire the content of communications.

Law enforcement officials may also be interested in the fine-grained data about household habits collected by the Smart Grid for a variety of reasons. As part of investigatory work to solve crimes, officials may want to establish or confirm the residence at an address at a certain critical time, and this information may be gleaned from smart meter reading data or temperature inside the home collected by a programmable thermostat. Law enforcement may also be interested in data collected by the Smart Grid that indicate illegal activities at home. For instance, access to smart meter reading data might be used in drug investigations, to enable law enforcement to learn about a suspect's marijuana growing cycle.[38] The privacy implications of law enforcement officials' interest in obtaining smart meter data suggest the need for strong legal protection of this information, especially because the Smart Grid data held by third parties as business records may not be subject to the same protections applicable to information kept within the home.[39]

---

[37] For instance, San Diego Gas and Electric (SDGE) uses the amount of the last SDGE bill to authenticate its customers when the customers sign up for an online account. *See* SDGE*, My Account*, https://myaccount.sdge.com/myAccountUserManager/pageflows/usermanager/Registration/begin.do.

[38] P.S. Subrahamanyam, David Wagner, Deirdre Mulligan, Erin Jones, Umesh Shankar, and Jack Lerner, CyberKnowledge and University of California at Berkeley, *Network Security Architecture for Demand Response/Sensor Networks*, June 2006, available at http://groups.ischool.berkeley.edu/samuelsonclinic/files/demand_response_CEC.pdf (under 3.2.4, Law Enforcement Practices) (hereinafter "Berkeley/CyberKnowledge Report").

[39] *See* Jack I. Lerner and Deirdre K. Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 Stan. Tech. L. Rev. 3.

IV. Legal and Policy Considerations

As seen above, Smart Grid information regarding a host of topics—appliance use, sleeping and eating habits, and even, with interpretation, movement within a residence—is directly reflective of highly personal activities that take place within the boundaries of the home—a location traditionally (and importantly) off-limits for investigations without strong procedural protections.

Under U.S. law, activities occurring within the sanctity of individuals' homes, because of their inherently personal nature, have been afforded special protection from intrusion by others.[40] The Supreme Court recently affirmed this strong protection for all types of data found in the home, noting in *Kyllo v. United States* that the "Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained…in the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."[41] In *Kyllo*, the Court invalidated the warrantless use of thermal imaging technology to measure heat emanating from a home as an unlawful search under the Fourth Amendment, despite the lack of any physical intrusion into the home by law enforcement.[42]

The implementation of Smart Grid technology creates concerns about the privacy of household activities that are qualitatively distinct from the existing infrastructure and data collection practices currently employed in the electrical grid.[43] While many of the implementation details are still under development, it is clear that Smart Grid systems may involve the retention by utilities and third-party service providers of large quantities of customer usage and demand response data on both a temporary and long-term basis. This section identifies several legal and policy issues warranting attention in discussing the implementation of Smart Grid technology.

a. Inadequacy of Current Privacy Rules

The consumer data implicated in the Smart Grid is governed by a patchwork of broad state and federal laws that may be generally applicable, but that neither specifically address the electrical grid nor were developed with Smart Grid technological advancements or business models in mind. In addition, at present, there is no federal consumer privacy law in the U.S. that might cover commercial activities related to Smart Grid information. Indeed, in the development of the Smart Grid Interoperability Standards, NIST recognized that a "lack of consistent and comprehensive privacy

---

[40] *See* Jack I. Lerner and Deirdre K. Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 Stan. Tech. L. Rev. 3.

[41] *Kyllo v. United States*, 533 U.S. 27, 37 (2001).

[42] *Id*. at 40.

[43] Berkeley/CyberKnowledge Report at 23.

policies, standards, and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use creates a privacy risk that needs to be addressed."[44] Rather than falling under a comprehensive single law, the Smart Grid intersects with a number of different federal and state rules regarding the privacy of activities occurring within the home, the handling of business records and identifiable customer information, the privacy of electronic communications, and access to computer systems.[45] Neither in isolation nor taken together do these existing laws provide adequate protection for the categories and quantities of data that may be generated by the Smart Grid.

Traditionally, the principal source of privacy regulation for electricity data has been state public utility commissions.[46] While some state public utility codes place explicit restrictions on the sharing of customers' personal information, these rules contain some regulatory uncertainty as to their coverage of Smart Grid data.[47] And generally, few state utility commissions have begun to consider the privacy implications of smart grid data.[48] General state laws governing business' and third parties' collection and use of consumers' personal data may apply to energy usage, but may be too narrow to cover the extensive and varied information generated by the Smart Grid. For example, the California Civil Code provides strong protections for personal or customer information maintained by utilities such as name, credit history, home address or phone number, but utility records that do not contain these types of personal information are not subject to the same protections.[49]

At the federal level, there is a similar patchwork of rules, which provides even less directly relevant guidance on the privacy protections applicable to the Smart Grid. The *Electronic Communications Privacy Act* (ECPA) sets out limitations on the interception of electronic communications and has been broadly applied to a range of communications systems. However, the greatest privacy issue with respect to Smart Grid data concerns what the utilities will do with the information they receive from their

---

[44] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0*,Sept. 2009, available at http://www.nist.gov/public_affairs/releases/smartgrid_interoperability.pdf, at 84.
[45] Berkeley/CyberKnowledge Report at 23.
[46] Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies*, May 9, 2009, available at SSRN: http://ssrn.com/abstract=1462285, at 24.
[47] See Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies*, May 9, 2009, available at SSRN: http://ssrn.com/abstract=1462285, at 17-22.
[48] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0*, Sept. 2009, available at http://www.nist.gov/public_affairs/releases/smartgrid_interoperability.pdf, at 84.
[49] Berkeley/CyberKnowledge Report at 25 (referencing CA Government Code § 6254.16).

customers, and ECPA places no limit on that. The Commission's Consumer Proprietary Network Information (CPNI) Rules, which require telecommunications carriers to obtain consumers' opt-in before using, disclosing, or permitting access to individually identifiable consumer information, do not necessarily directly bear on the privacy issues surrounding a Smart Grid information network.[50] However, as the transmission of Smart Grid services grows increasingly complex and more communications-based, utilities may find themselves subject to laws governing telecommunications providers, meaning they would be bound by some privacy protections on data related to their service.[51] The *Computer Fraud and Abuse Act* (CFAA), which governs unauthorized access to computer systems, may also be relevant, under a broad construction, to regulate invasions of the Smart Grid. Unauthorized access to obtain information from or cause damage to devices like smart meters, wireless sensors, smart appliances, and a consumer's home computing system might generate liability under an expansive reading of the CFAA.[52] Finally, the Federal Trade Commission (FTC) likely has general jurisdiction under Section Five of the FTC Act to pursue actions against Smart Grid entities engaging in "unfair and deceptive trade practices," such as, for example, failing to adopt, disclose, or adhere to reasonable privacy and security practices.[53]

This introductory discussion of the rules possibly applicable to Smart Grid technologies reveals the disjointed and outdated nature of current consumer protections for energy data. Industry lacks a clear set of privacy principles to govern Smart Grid technologies. A cohesive approach—including perhaps a regulatory framework—that reflects the realities of an interconnected and digitized electricity grid in which consumers are active contributors of personal data, is needed. NIST's suggestion that we need further privacy impact assessments on changes to data collection and data flows and processing prompted by the implementation of the Smart Grid is a sensible starting point in developing this harmonized approach.[54]

b. Key Privacy and Security Considerations in Developing Smart Grid Rules

An effective regulatory regime for the data collected and utilized in the Smart Grid must contain explicit privacy protections for the consumer information likely to be exchanged among consumers, utility companies, and third-party service providers. The

---

[50] Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies*, May 9, 2009, available at SSRN: http://ssrn.com/abstract=1462285, at 25-26.
[51] Mark Foley, *Data Privacy and Security Issues for Advanced Metering Systems,* SmartGridNews.com, July 1, 2008.
[52] 18 USC § 1030; *See also* Berkeley/CyberKnowledge Report at 28.
[53] *See* Mark Foley, *Data Privacy and Security Issues for Advanced Metering Systems*, SmartGridNews.com, July 1, 2008.
[54] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0*, Sept. 2009, available at http://www.nist.gov/public_affairs/releases/smartgrid_interoperability.pdf, at 84.

widely recognized and adopted Fair Information Practices principles[55] provide a valuable framework for choosing key privacy rules to govern the data collection, use, and storage issues presented by the Smart Grid.[56] Such protections might include:

- **Transparent notice to the consumer of data collection practices**. Utilities and companies developing Smart Grid devices should develop privacy policies clearly stating what information will be collected from and about their homes and home activities, who will receive the information, and the purposes it will be used for.

- **Minimized data collection, access, and retention**. Utilities and third-party technology providers should limit data collection to the minimum amount necessary to support the purpose for which the consumer is providing data. Further, access to granular data about consumers' energy usage should be limited within a utility to entities with a justifiable requirement for the data, such as a billing department. Policies governing the retention of customers' utility records, which widely reflect the industry standard of a seven-year retention period,[57] should be re-evaluated in light of the transition to the Smart Grid and the attendant enhanced collection of consumer data.

- **Meaningful consumer choice regarding use and disclosure of information.** Consumers should provide informed consent before information about their energy usage is used for a purpose materially different from what it was collected for or is transferred to third parties, including those providing a consumer web interface for managing energy use. An opt-in consent, after clear notice of the use has been provided, is likely the most appropriate standard, although the issue warrants more examination. Comprehensive privacy protection of consumer data also requires that utilities impose the same restrictions they adhere to on contractors' use of consumer data.

- **Consumer access to usage information**. Customers should be provided with reasonable access to all usage information from their utilities or third-party providers, and should have the opportunity to dispute or make corrections to such data as appropriate.

---

[55] *See* Organization for Economic Co-operation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Sept. 1980, available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[56] *See* Berkeley/CyberKnowledge Report. *See also* Mark Foley, *Data Privacy and Security Issues for Advanced Metering Systems,* SmartGridNews.com, July 1, 2008; Susan L. Lyon, *Greening of it: Privacy Challenges Could Stall Smart Grid*, Sustainable Industries, June 1, 2009.

[57] *See* Berkeley/CyberKnowledge Report at 32.

- **Security controls and remedies for unauthorized use**. Utilities and third-party service providers must establish strong technical and procedural mechanisms to protect consumers' personal data from unauthorized collection and use, both internally and externally. These mechanisms should be tested through an independent auditing process, and consumers should have remedies in the event of misuse or unauthorized access.

c. Key Privacy and Security Considerations in Developing Smart Grid Technologies

Beyond legal and contractual rules, new Smart Grid technologies should be engineered to protect privacy from the early design and planning stages. The Commission's Notice requests input regarding the suitability of various communications technologies for the Smart Grid. In considering these technologies, we emphasize the importance of ensuring that privacy is integrated into every point in the network involving the collection, access, and transfer of consumer information.[58] Addressing privacy issues during the process of technical design and implementation provides an opportunity to maximize the benefits of new technologies while minimizing privacy risks, and helps avoid the difficulty and expense of retrofitting a completed network with new safeguards. Two specific illustrations of this "Privacy by Design" principle include[59]:

- **Designing the Smart Grid communications network to ensure the privacy of data transmissions.** This includes implementing encryption over the entire data transmission path, from the meter to the utility, unless there are well-justified cases in which encryption is not necessary to protect consumer privacy.[60] Given that serious privacy and security risks from outside attacks are likely to occur in the transmission network because of the opportunity to compromise data from many households rather than a single meter, it is sensible to secure the network as a threshold matter, with additional security implemented as appropriate. This point should be taken into account in considering responses to Question 1(a) and Question 3(f.iv).

---

[58] Mark Foley, *Data Privacy and Security Issues for Advanced Metering Systems*, SmartGridNews.com, July 1, 2008.

[59] For further development of these and additional technological recommendations for protecting privacy in the short, medium and long-term Smart Grid deployments, *see* Berkeley/CyberKnowledge Report at 76-78.

[60] Generally speaking, it is well established that proprietary formats are insufficient to secure sensitive data compared to well-studied and time-tested standard algorithms. *See* Berkeley/CyberKnowledge Report at 83-84.

- **Minimizing the amount of consumer data that leaves the house**. As meters become more capable of sophisticated computation, it may be possible to localize the collection, use and storage of private data at the point of consumption, so that billing, for example, might occur within the home. Aggregation and anonymization processes could then be used to enable the transmission of only relevant abstractions of data. This would maximize the consumer's control over the use and reuse of data, while limiting exposure to the unauthorized access or misuse of data more likely to occur outside of the home.[61] This point should be taken into account in considering responses to Questions 5(a) and 5(b).

V. Conclusion

As the Commission proceeds with its review of the implementation of Smart Grid technology as part of the development of the National Broadband Plan, privacy issues should be thoughtfully addressed in both the regulatory and technological spheres.

Designing legal rules and building technologies that protect consumers from the inappropriate collection and misuse of specific energy data that reveals intimate aspects of home life will help spur consumer confidence in, and demand for, the Smart Grid. Conversely, the failure to adequately address privacy issues or other violations of consumer expectations about the appropriate use of their data may result in strong opposition to Smart Grid schemes. If the public does not trust the new grid, it may not even develop to a stage where we can test its true effectiveness. Focusing attention now on the privacy issues implicated in the Smart Grid is critical if we are to position ourselves to fully realize the consumer benefits of a modernized and greener grid.

/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

[61] *Id*. at 78, 87.

We are grateful for the Commission's attention to this important issue, and look forward to providing any further information that may be useful.

Respectfully submitted,

Jennifer M. Urban
Elizabeth Eraker
Longhao Wang

Samuelson Law, Technology & Public Policy Clinic
UC Berkeley School of Law
Berkeley, CA 94720-7200
(510) 642-7338

on behalf of:
Center for Democracy & Technology

October 2, 2009