Before the
Department of Commerce

National Institute of Standards and Technology

Request for Comments	)	
	)	
Draft NIST Interagency Report (NISTIR)	)	Docket Number 0909301329-91332-01
7628, Smart Grid Cyber Security Strategy	)	
And Requirements	)	

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

December 1, 2009

Jennifer M. Urban
Elizabeth Eraker
Longhao Wang

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

on behalf of the
Center for Democracy & Technology

December 1, 2009

Table of Contents

Executive Summary

We are grateful for and commend NIST's vitally important work in developing a Smart Grid Cyber Security strategy, and particular the effort to make recommendations for protecting consumer privacy, in the *NIST Interagency Report (NISTIR) 7628.*

The Smart Grid promises great benefits to consumers and the environment. At the same time, it presents new risks to privacy in its enhanced collection and use of highly granular consumption data, which can reveal intimate details about activities within the home. The entrance of new entities and technologies delivering energy services, the speed at which this new infrastructure is being deployed, and the lack of clear governing rules further support the need to address the privacy risks to consumers created by the Smart Grid.

As part of NIST's work to coordinate the development of a framework for a modernized and interconnected grid, it should develop and recommend strong privacy principles that can be incorporated into standards and technical requirements, and should develop robust, rigorous use cases that illustrate privacy-affecting scenarios in Smart Grid technologies and services, and show how privacy principles can be built into Smart Grid architecture. Creating privacy-protective systems and technologies for the Smart Grid should not require a tradeoff with functionality, but it will require thoughtful design. In adopting a "privacy by design" approach, rather than attempting to tack on privacy at a later point, NIST can support the most effective means of protecting consumer privacy in the Smart Grid, and provide needed guidance to state regulators and industry players.

Developing effective privacy protections for the Smart Grid must be grounded in a thorough examination of how the proposed technologies will affect consumer privacy interests. In this Comment, we provide an overview of consumer data flow in the Smart Grid under several proposed NIST standards and discuss the privacy risks and legal rules implicated by the unprecedented collection of detailed information about customers' energy and appliance use contemplated by Smart Grid technologies and services—information traditionally afforded strong legal protection within the home. We proceed to propose a specific framework for protecting privacy in the Smart Grid based on a robust and comprehensive set of Fair Information Practice Principles ("FIPPs"), including who should be covered, what types of data should be covered, and how a FIPPs-based framework can ensure meaningful protections for consumers' "Household Energy Data." All of the technical standards identified by NIST for implementation in the Smart Grid should be evaluated against these principles, and NIST should make recommendations regarding standards based upon them, and upon a rigorous set of use cases that can inform standards bodies and the design of new Smart Grid technologies.

Before the
Department of Commerce

National Institute of Standards and Technology

Request for Comments	)	
	)	
Draft NIST Interagency Report (NISTIR)	)	Docket Number 0909301329-91332-01
7628, Smart Grid Cyber Security Strategy	)	
And Requirements	)	

Comments of the Center for Democracy & Technology

December 1, 2009

The Center for Democracy & Technology ("CDT") respectfully submits these comments in response to the National Institute of Standards and Technology's ("NIST") request for comments on the *Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy and Requirements* ("Draft"). CDT is a nonprofit, public interest organization dedicated to preserving and promoting openness, innovation and freedom on the decentralized Internet**.**

I. Introduction

NIST's work to develop a Smart Grid cybersecurity strategy, including recommendations for protecting consumer privacy in the modernized grid, is a vitally important effort. The transition to the Smart Grid promises great benefits for consumers, including lowered energy costs, increased usage of environmentally-friendly power sources, and enhanced security against attack and outage. At the same time, it presents new risks to consumer privacy. At the core of the modernized grid's functionality is fine-grained household data; in order to enable more efficient energy use, and to more actively engage individual consumers and their appliances in energy management, the Smart Grid, as currently envisioned by proponents, depends on the collection and use of highly granular consumption data.[1] Recent experiments using the simplest data mining and pattern matching techniques reveal how easily this information can be analyzed to expose intimate details about activities within the home with a high degree of accuracy.[2]

[1] Patrick McDaniel and Stephen McLaughlin, *Security and Privacy Challenges in the Smart Grid*, IEEE, May/June 2009.
[2] Mikhail Lisovich, Deirdre K. Mulligan, and Stephen B. Wicker, *Privacy Concerns in Upcoming Demand-Response Systems*,
http://wislsrv.ece.cornell.edu/~mikhail/Copy%20of%20Source%20Material/lisovich2007pci_v3.pdf.

From a consumer privacy perspective, we stand at a critical juncture in the development of Smart Grid technologies for several reasons. First, the emergence of increasingly sophisticated metering technologies are enabling the unprecedented collection of energy consumption data, removing a "latent structural limitation" that previously protected the revelation of intimate details about household activities.[3] Whereas historically a consumer's consumption data may have been collected once a month or less frequently from a traditional meter fixed to the side of a house, in the Smart Grid, sophisticated new demand response systems will collect a record of 750 to 3,000 data points a month, revealing variations in consumption that can reflect specific household activities such as sleep, work, and travel habits.[4] Second, the transition to a highly-interconnected and less-bordered electrical infrastructure is inviting participation by new entities, such as third-party service providers offering new web-based portals for managing energy use, who are utilizing consumer data in new ways and presenting the need for privacy analysis extending beyond the more straightforward consumer-to-utility relationship. Third, the rapid pace of Smart Grid deployment, and the speed at which new Smart Grid technologies are moving out of the pilot project stage to large-scale implementation, is making the consideration of the consumer privacy issues presented by these technologies more urgent. Finally, against this landscape of rapid development, there remains a "lack of consistent and comprehensive privacy 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," creating "a privacy risk that needs to be addressed," as prudently noted in the NIST Draft.[5]

Against this backdrop, NIST's work to coordinate Smart Grid standards will ensure there is a common set of widely supported open protocols governing the modernized grid. But there is also an urgent need for NIST to issue recommendations based on strong privacy principles that can be reflected in these technical standards and requirements. Adopting a "privacy by design" approach, and building standards that reflect privacy interests, rather than attempting to tack on privacy at a later point, is the most effective means of protecting consumer privacy and security.[6] Embedding privacy protections into the technology now, before smart meters and other Smart Grid technologies are fully deployed, and as information systems are being developed, will also 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.

---

[3] *See* Harry Surden, *Structural Rights in Privacy*, 60 SMU Law Review 1605 (2007), http://ssrn.com/abstract=1004675, at 139 (noting how "the widespread diffusion of an emerging technology effectively causes a rights-shift with respect to privacy interests protected by latent structural constraints").
[4] 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. at 3.
[5] NIST, *Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements*, http://www.nist.gov/smartgrid/.
[6] *See* Information and Privacy Commissioner of Ontario, *Privacy by Design*, http://www.privacybydesign.ca/.

Further, ensuring that a robust set of privacy principles underlie NIST's Smart Grid framework is important in providing guidance to state regulators, utilities, third-party service providers, and device manufacturers wrestling with privacy issues. California, for example, recently amended its Public Utility Code to require the Public Utility Commission to explicitly consider NIST standards as a candidate for implementation in the State's Smart Grid infrastructure.[7]

We commend NIST's efforts to date to consider the privacy implications of the consumer-to-utility information collection envisioned in the Smart Grid, and especially the work of the Cyber Security Coordination Task Group ("CSCTG") in performing an initial Privacy Impact Assessment ("PIA") of that collection in the *Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy and Requirements* document ("Draft"). However, much work remains to be done. Developing effective privacy protections for the Smart Grid must be grounded in a rigorous examination of how the proposed technologies will affect consumer privacy interests.

In this Comment, we provide an overview of consumer data flow in the Smart Grid under several standards identified by NIST for implementation, discuss the privacy risks and legal rules implicated by these technologies, propose a specific framework for further developing privacy protective principles that should be reflected in the technical standards and requirements ultimately recommended by NIST, and call for the rigorous development of relevant use cases that can inform standards bodies and technology design. While our Comment generally addresses the standards proposed in the NIST Draft Framework and Roadmap, 1.0 ("Framework"),[8] we focus specific attention on the discussion of consumer privacy and applicable principles in Chapter Two of NISTIR 7628, "Privacy and the Smart Grid."

II. Smart Grid Consumer Data Flow and Applicable Standards Identified by NIST for Implementation

A. Overview

We appreciate NIST's recognition that for customer-to-utility data flow, "the specific data items involved, and associated privacy issues, are very different" from the types of data flows between commercial meters and utilities.[9] In this section, we review and summarize data flow in the Smart Grid that implicates consumer privacy, especially consumer privacy within the home, and that is either presently covered by standards

[7] California Senate Bill 17, http://info.sen.ca.gov/pub/09-10/bill/sen/sb_0001-0050/sb_17_bill_20091011_chaptered.html (signed Oct. 11, 2009).
[8] 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.
[9] NIST, *Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements*, http://www.nist.gov/smartgrid/, at 11.

identified for implementation by NIST, or available in representative products and services currently on the market. While we cannot be comprehensive, this data flow analysis conveys a basic picture of Smart Grid data flow, as implemented in existing standards and technologies.

Currently, smart meters comprise about 4.7%, or 6.7 million, of all electricity meters in the U.S., and the Department of Energy projects that 52 million more smart meters will be installed by 2012.[10] Using stimulus funds allocated to the modernization of the electrical grid, the Administration recently announced Smart Grid grants of $3.4 billion dollars to fund the implementation of smart meters in 18 million homes.[11] At the same time, manufacturers are working to roll-out "smart" versions of household appliances over the next several years, which will be capable of communicating with smart meters and other appliances, and directly with utilities in some instances.[12] In addition, consumers can purchase and install their own metering devices that monitor energy consumption of a home or an individual device in close to real time.[13]

As widely noted, 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 consumers 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 later hour. This "demand response" process improves energy efficiency by reducing peak demand, and at the same time, may reduce consumer's energy bills. [14] Other major benefits of the transition to the Smart Grid, not directly related to consumer information, include reducing greenhouse gases by allowing the efficient use of clean energy sources and enhancing grid defenses against attack and outage.

The increased flow of data related to customers' homes in the Smart Grid exemplifies a paradigm shift from the traditional customer-to-utility data flow. First, the Smart Grid entails much more granular data collection compared to historical practice—all Smart Grid technologies contemplate or actively rely on the collection of energy consumption data at much shorter time intervals than historically collected from household consumers, down to real-time or near real-time. Second, Smart Grid

---

[10] 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 14.
[11] Rick Merritt, *U.S. awards $3.4 billion in smart grid grants*, EEtimes.com, http://www.eetimes.com/news/design/showArticle.jhtml?articleID=220900617.
[12] Department of Energy, *Smart Grid System Report*, www.oe.energy.gov/DocumentsandMedia/SGSRMain_090707_lowres.pdf.
[13] *See, e.g.,* TED 500, http://www.theenergydetective.com/ted-5000-features.html.
[14] 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.

technologies may allow utilities to collect electricity consumption data for a single, uniquely identified home appliance, while historically, utilities have only collected aggregate electricity consumption data of all appliances within a household. Third, a much greater variety of information is collected by Smart Grid technologies than has been collected by conventional energy services. Utilities may collect not only energy consumption data, but also unique identifiers and functionality of home appliances, temperature inside the home, and location information of plug-in hybrid electric vehicles in the Smart Grid, just to name a few. Finally, third-party entities that will have access to customers' private data, such as Google PowerMeter and Microsoft Hohm, have entered the energy marketplace.

To illustrate these changes, consider Pacific Gas & Electric's ("PG&E") SmartAC program, in which the utility company installs programmable thermostats for consumers' air conditioners, which communicate directly with the utility.[15] PG&E might use the communication channel to display messages on the screen of the thermostat, such as weather warnings, greetings, and system maintenance notices.[16] Consumers can also configure their thermostats on PG&E's website,[17] giving the utility company information about consumers' temperature preference in their homes. It is possible that utilities 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 a consumer chooses to register other smart appliances or a home area network (HAN) with the utility company in order to enroll in certain utility-sponsored programs, detailed information about those appliances or the HAN could also be collected by the utility.[18] Utilities may remotely turn off consumers' registered devices,[19] or instruct consumers' devices to shed load.[20] Furthermore, if a consumer is interested in using a third-party service to monitor usage, such as a web interface offering a visualization of energy use through a graphical display, the consumer can authorize a provider such as Google PowerMeter to collect smart meter data directly from utilities.[21]

---

[15] PG&E, *SmartAC Frequently Asked Questions: What are the SmartAC technology options?,* http://www.pge.com/myhome/saveenergymoney/energysavingprograms/smartac/faq/.
[16] PG&E, *Honeywell Thermostat Operating Manual*, http://www.pge.com/includes/docs/pdfs/shared/smartac/thermostatuserguide.pdf.
[17] PG&E, *SmartAC Thermostat Programming Website Guide,* http://www.pge.com/includes/docs/pdfs/shared/smartac/pg-wc-7e_webguide_tstat[f]-screen.pdf.
[18] *See, e.g.*, UtilityAMI, *Home Area Network System Requirement Specification, 2.2.10*; Southern California Edison, *SmartConnect Use Cases C5*, http://www.sce.com/NR/rdonlyres/EC46A2AC-9D43-4674-90A7-CBE47F362CDE/0/C5_Use_Case_090105.pdf.
[19] For example, in Florida Power and Light Company's Residential On Call program, the utility company can remotely turn off customers' registered devices at critical times in exchange for a monetary reward to the customers. *See* http://www.fpl.com/residential/savings/oncall.shtml.
[20] ZigBee Alliance, *ZigBee Smart Energy Profile Specification*, D.2.2.3, "Load Control Event," at 141.
[21] Google PowerMeter utility partners, http://www.google.org/powermeter/partners.html.

This paradigm shift in data flow undermines key assumptions underlying existing privacy laws and regulations and imposes considerable privacy risks on customers, as we further explore below. Privacy principles developed for the Smart Grid should be grounded in a thorough review of the data flow implicating consumer privacy, including an analysis of how consumer data is being collected, used, and retained by various entities under the standards identified for implementation. We hope the information presented in this Comment may assist NIST in that effort.

B. Data Flow in Standards Identified by NIST for Implementation

Under the Energy Independence and Security Act (EISA) of 2007, NIST is charged with the responsibility to "coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems." In September 2009, NIST published its *Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, which identified 31 existing standards that could be implemented in the Smart Grid. Of the standards identified for implementation by NIST, the standards related to demand response and to the Home Area Network (HAN) directly involve demand-side energy management of consumer appliances and implicate consumer privacy issues. As such, we explore some of these standards here: the ZigBee/HomePlug Smart Energy Profile, Open Automated Demand Response (OpenADR), and OpenHAN. [22] We note that this is by no means a comprehensive list of standards that may affect consumer privacy in the Smart Grid—many other aspects of architecture and practice will be relevant, as well. We include these below because of their direct relevance to consumer interaction with the Smart Grid and their obvious implications for privacy.

1. ZigBee/HomePlug Smart Energy Profile

The ZigBee/HomePlug Smart Energy Profile is jointly developed by ZigBee Alliance and HomePlug Powerline Alliance members and was selected by NIST as an interoperable standard for HAN devices and communications. It is created to "further enhance earlier HAN specifications (specifically, the ZigBee Alliance Smart Energy Profile, v 1.0)"[23] and "serves as the basis for a following Technical Requirements Document (TRD), which is the next step in line with creating the actual specification."[24] Although the ZigBee/HomePlug Smart Energy Profile includes a variety of use cases and its Technical Requirements Document is still being developed, important details about its implementation can be gleaned from the ZigBee Alliance Smart Energy Profile

[22] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, 1.0*, at 34.
[23] ZigBee Alliance and the HomePlug Alliance, *ZigBee/HomePlug Smart Energy Profile*, http://www.zigbee.org/Markets/ZigBeeSmartEnergy/ZigBeeSmartEnergyOverview/tabid/431/Default.aspx, at 3.
[24] *Id*. at 1.

Specification, v 1.0, [25] upon which the ZigBee/HomePlug Smart Energy Profile is based. The information below is based on our review of ZigBee Alliance Smart Energy Profile Specification, version 1.0.

A ZigBee Smart Energy network may consist of an Energy Service Portal (ESP), Metering Device, Programmable Communicating Thermostat (PCT), and Smart Appliance Device.[26] The ESP serves as the gateway that connects the utilities' communications network to the consumers' Smart Appliance Devices. The ESP may be installed within a meter, thermostat, In-Premise Display, or as a standalone device. A consumer's devices must join the ZigBee Smart Energy network to communicate with the ESP, other devices on the network, or the utility. Within a ZigBee Smart Energy network, the ESP communicates with customers' devices via encrypted wireless communication.

To join a Smart Appliance Device, such as a washing machine or refrigerator, to a ZigBee Smart Energy network and communicate securely with the ESP of the network, a customer needs to register the Smart Appliance Device with the utility. The registration process requires the customer to provide the utility with the 64-bit device identifier[27] that uniquely identifies the Smart Appliance Device, the first 24 bits of which could uniquely identify the manufacturer of the device.[28] The device identifier is conveyed from the customer to the utility via an out-of-band mechanism such as a telephone call, or web site registration. The utility then uses the device identifier to create keys for secure communication between the ESP and the joining Smart Appliance Device.[29] The device identifier may also be used by the ESP to maintain a list of authorized devices for a particular HAN.[30]

Metering information, including electric, gas, water, and potentially thermal consumption data, of smart devices may be collected by the ESP and potentially revealed to the customer's utility. Metering Devices may be fitted with Smart Appliance Devices, and measure energy usage at the device level.[31] In the design of ZigBee Smart Energy Profile Specification, Metering Devices and Programmable Communicating Thermostats (PCT) are all directly connected to the ESP.[32] Since the ESP is often embedded in smart

---

[25] ZigBee Alliance, *ZigBee Smart Energy Profile Specification*, available at http://www.zigbee.org/DownloadZigBeeTechnicalDocuments/tabid/310/Default.aspx
[26] *Id*. at 71-77.
[27] *Id*. at 115.
[28] Wikipedia, Organizationally Unique Identifier, http://en.wikipedia.org/wiki/Organizationally_Unique_Identifier#64bit_Extended_Unique_Identifier_.28EUI-64.29 (last visited Dec. 1, 2009).
[29] ZigBee Alliance, *ZigBee Smart Energy Profile Specification*, http://www.zigbee.org/DownloadZigBeeTechnicalDocuments/tabid/310/Default.aspx, at115.
[30] *Id*. at 56.
[31] *Id*. at 72.
[32] *Id*. at 162-64.

meters that communicate with the utilities,[33] utilities could easily obtain metering information from Metering Devices or PCTs, revealing the energy usage of individual Smart Appliance Devices or the temperature inside customers' homes.

The demand response and load control commands in the ZigBee Smart Energy Profile Specification could reveal the functionality of customers' Smart Appliance Devices. The ZigBee standard defines 12 Device Classes, including water heater, interior/exterior lighting, electric vehicle, and spa.[34] Each Smart Appliance Device is assigned a Device Class by the device manufacturer. In a demand response or load control event, a command from the utility indicates the class of devices needing to participate in the event.[35] The Smart Appliance Device may report event participation in a unique manner as defined by the device manufacturer,[36] or ignore the event if the Device Class of the Smart Appliance Device does not match the Device Class in the command.[37] Therefore, utilities could easily identify the Device Class of a Smart Appliance Device inside a customers' home from the response the utilities receive to demand response and load control commands. For instance, if a utility sends a load control command indicating a customer's water heater needs to "reduce its average load by 10 percent"[38] and receives a response from the customer's ESP confirming participation in the event, the utility could easily tell that the customer has a water heater.

As such, technologies developed under the Zigbee standard could collect and communicate far more detailed information than has been collected in the past, and use of these technologies could result in information about the intimate life of a household leaving the home and being stored outside of it, in utilities' or other providers' systems.

2. Open Automated Demand Response (OpenADR)

The Open Automated Demand Response Communication Specification (OpenADR), developed by Lawrence Berkeley National Laboratory, is a communications data model[39] designed to facilitate automating demand response actions at the customer location.[40] OpenADR has been used in over 200 facilities in California[41] and has been

---

[33] PG&E, SDGE and SCE all have HAN gateway embedded in smart meters. *See* Home Area Network (HAN) Overview, Pacific Gas & Electric Company, Jan. 2009, www.edisonfoundation.net/iee/issueBriefs/PG&E_HAN_January_2009.pdf.
[34] ZigBee Alliance, *ZigBee Smart Energy Profile Specification*, http://www.zigbee.org/DownloadZigBeeTechnicalDocuments/tabid/310/Default.aspx, at143.
[35] *Id*. at 148.
[36] *Id*. at 157.
[37] *Id*. at 143 (noting that "if the Device Class and/or Utility Enrolment Group fields don't apply to your End Device, the Load Control Event command is ignored").
[38] *Id*. at 141.
[39] Demand Response Research Center, *CEC OpenADR-Version 1.0 Report*, at http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf, at1.
[40] *Id*. at 2.
[41] *Id*. at 6.

identified by NIST as one of the Smart Grid standards available for implementation.[42] In contrast to the ZigBee/HomePlug Smart Energy Profile, which aims to enable "communication between utility companies and everyday household devices,"[43] OpenADR was initially developed to "provide interoperable signals to building and industrial control systems"[44] and is currently used by large businesses in California with centralized energy management systems.[45] However, OpenADR has also been successfully deployed in residential settings[46] and Programmable Communicating Thermostats (PCTs) are being developed to allow residential facilities to participate in OpenADR programs.[47]

In the OpenADR architecture, the Demand Response Automation Server (DRAS) is the intermediary for the communication between the utility and consumer.[48] The DRAS may be a standalone third-party service, or integrated with the utility or consumer's information system.[49] A DRAS Client is a device on the customer's premise that communicates with the DRAS.[50] OpenADR mandates that all public communication interfaces be subject to confidentiality, integrity, authentication and non-repudiation

---

[42] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.*

[43] ZigBee Alliance and the HomePlug Alliance, *ZigBee/HomePlug Smart Energy Profile*, http://www.zigbee.org/Markets/ZigBeeSmartEnergy/ZigBeeSmartEnergyOverview/tabid/431/Default.aspx, at 1.

[44] Demand Response Research Center, *CEC OpenADR-Version 1.0 Report*, http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf.

[45] *See* Southern California Edison, *Fact Sheet: Automated Demand Response*, http://www.sce.com/NR/rdonlyres/08EBB404-C15D-4FD1-ABBD-E364A82C2A57/0/2008_0201_AutoDRFactSheet.pdf (stating that "Auto DR Program is open to customers with demands equal to or greater than 200 kW who either have an Energy Management System (EMS) that is active or can be reactivated, or are willing to install an EMS"); PG&E, Auto-DR: How it Works, http://70.32.94.23/Auto-DR/pge_how_it_works.html (stating that "Auto-DR is appropriate for many commercial, industrial, and agricultural sites with billed maximum demand of 200 kW or greater").

[46] Tendril, *Tendril Achieves First Open ADR Compliant Platform,* http://www.tendrilinc.com/2009/01/tendril-achieves-first-open-adr-compliant-platform-2/ (stating that "Tendril Residential Energy Ecosystem (TREE) Platform could automatically shed residential loads upon receiving critical peak pricing and real-time pricing messages from an OpenADR compliant server").

[47] Demand Response Research Center, *CEC OpenADR-Version 1.0 Report*, http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf (stating that "Programmable Communicating Thermostats (PCTs) are currently being developed that in the future may allow small commercial and residential facilities to participate in DR programs"), at APD-56. *See id.* at 3 (stating that the "Demand Response Research Center will also continue to evaluate end-use DR control strategies for homes, large and small commercial buildings, and industrial facilities").

[48] Demand Response Research Center, *CEC OpenADR-Version 1.0 Report*, http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf, at14.

[49] *Id.* at 33 (noting "in the architecture…that the DRAS itself is depicted as a standalone service…this is the most general case… [and that] specific incarnations of the DRAS may be integrated within either the utility or participant's IT infrastructure and services"). An example of a DRAS is the Akuacom DRAS, which "accepts DR events and tariff information from utilities and ISO's and turns these into standardized OpenADR signals that are sent to Energy Management Systems (EMS) at participant facilities." Akuacom, Solutions, http://www.akuacom.com/solutions/index.html.

[50] *Id*. at APD-4.

requirements, and has identified a minimum level of cipher suit for DRAS, which includes standards for key exchange, data encryption, message integrity and message authentication.[51] The OpenADR identifies its opt-out functionality as one of its defining features,[52] and requires that customers can opt out of a demand response program at any time.[53]

The OpenADR standard contains seven use cases,[54] and each use case covers three broad scenarios: configuration, execution, and maintenance.[55] For our purposes, we extract one-directional customer-to-DRAS, DRAS-to-utility, and customer-to-utility data flow from the use cases and scenarios.

Customers, or the DRAS Client on a customer's premise, provide the following information to the DRAS:

- Configuration information used to set up a connection with the DRAS, including identification and password of the customer and the DRAS Client, IP connection information, and the customer's contact information.[56]
- Customer's bid for load reduction, if the customer participates in the utility's bidding program.[57] After the customer receives a request for bids from the utility, the customer may submit a bid to the DRAS.[58] Customers may adjust or cancel their current bid.
- Feedback information from the DRAS Client to the DRAS when a demand response or bidding event is executed. The feedback information includes customer ID, near-real-time load, amount of load reduction, and load reduction end uses (e.g. HVAC or lighting).[59]
- Optionally, the load reduction potential of the customer.

The DRAS provides the following information to the utility:

---

[51] *Id*. at 113-116.
[52] *Id*. at 2.
[53] Demand Response Research Center, *CEC OpenADR-Version 1.0 Report*, http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf, at 28.
[54] *Id*. at Appendix D.2.
[55] *Id*. at 18.
[56] *Id*. at 25.
[57] OpenADR use cases contains two bidding programs: Demand Bidding Program, which pays an incentive to reduce electric load according to a voluntary bid made for a scheduled load reduction, and Capacity Bidding Program, which pays customer a monthly incentive to reduce load to a pre-determined amount. *Id*. at APD-12, APD-23.
[58] Demand Response Research Center, *CEC OpenADR-Version 1.0 Report*, http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf, at 28 (D.2.2, Demand Bidding Program, APD-15).
[59] *Id.* at 27. *See also* http://openadr.lbl.gov/src/FeedBack.xsd (a formal description of feedback information in XML Schema).

- Customer's standing bid, if the customer participates in the utility's bidding program.[60]
- Feedback information from the DRAS Client.
- Optionally, load reduction potential based upon all customers in program.

The utility also measures customers' electricity usage, but the details of the process are beyond the scope of the OpenADR standard.[61]

Under the OpenADR standard, utilities do not interact directly with customers' HAN devices, but interact with customers' energy management system. This design has three implications: first, to use OpenADR, customers must have their own energy management system that translates demand response signals from utilities to actionable instructions for Home Area Network devices (HAN devices).[62] Second, utilities collect far less information about customer's devices under OpenADR than under the ZigBee Smart Energy Profile Specification. For instance, customers do not need to register their HAN devices with utilities, since the utilities do not directly communicate with customers' HAN devices but with customers' energy management systems. Third, utilities exert less control over customers' HAN devices. For instance, instead of a command instructing customers' water heaters to reduce load by 10%, as is contemplated by the ZigBee Smart Energy Profile Specification,[63] an OpenADR command would only instruct a consumer's energy management system to reduce load[64] and then the consumer's energy management system would decide how to respond.

3. OpenHAN

The OpenHAN standard identified by NIST for implementation is the collaboration of more than a dozen investor-owned North American utilities and reflects utilities' view of the Home Area Network. It is a high-level policy statement rather than a requirements document.[65]

Similar to the ZigBee Smart Energy Specification, OpenHAN has use cases in which a HAN device is registered with the utility[66] and communicates with the utility via the Energy Service Interface, which may be embedded in smart meters.[67] In addition, OpenHAN has also included an Energy Management System (EMS) that receives

[60] *Id*. at APD-18.
[61] *Id.* at APD-6.
[62] The Tendril Residential Energy Ecosystem (TREE) Platform may already fulfill this function. *See* Tendril, Tendril Achieves First Open ADR Compliant Platform, Jan. 29, 2009, http://www.tendrilinc.com/2009/01/tendril-achieves-first-open-adr-compliant-platform-2/.
[63] ZigBee Alliance, *ZigBee Smart Energy Profile Specification*, http://www.zigbee.org/DownloadZigBeeTechnicalDocuments/tabid/310/Default.aspx, at B.1.
[64] For a formal specification of commands under OpenADR, see http://openadr.lbl.gov/src/EventInfo.xsd.
[65] UtilityAMI, *OpenHAN System Requirement Specification*, at 9.
[66] *Id*. at 71.
[67] *Id.* at 27.

notification from utilities and controls connected HAN devices.[68] The EMS may be offered by third parties;[69] however, the utility may still require HAN device registration in the Energy Management use case for reliability programs, according to OpenHAN.[70]

C. Data Flow in Real-World Products

We provide here some background on the role third party service providers are likely to play in the collection and use of consumer energy data in the Smart Grid. These products mainly include third-party web portals, consumer devices and Home Area Network vendors.

Third-party web portals, such as Google PowerMeter and Microsoft Hohm, collect customers' smart meter reading data. Third-party web portals may enter into partnership with utilities, and obtain customers' smart meter reading data from the utilities. The frequency of these readings may depend on customers' utility.[71]

Third-party web portals may also obtain customers' meter reading data from metering devices that customers purchase. For instance, one of Google PowerMeter's device partners, a company called TED (for "The Energy Detective"), uses "clip-on current transformers"[72] that can measure electricity consumption of a home, or an individual device,[73] with accuracy within 2%.[74] The electricity consumption data is collected in real-time and relayed to a customer gateway device via ZigBee wireless communication. The customer gateway device then provides the data to a stand-alone device or computer to be displayed to the customer, or provides the data to Google PowerMeter every 10 minutes if the gateway is connected to the Internet.[75]

Third-party web portals may also solicit customers to provide information about their homes via the web portal. For example, Microsoft Hohm encourages customers to provide detailed information about their home in order for Hohm to make energy-saving recommendations to customers. Information that Hohm solicits includes the heating

---

[68] *Id*. at 62.
[69] *Id*. at 28.
[70] UtilityAMI, *OpenHAN System Requirement Specification,* at 62 (noting that the "use case does not imply the Utility's preferred configuration or communication for reliability programs," meaning that the utility may still require HAN device registration).
[71] Google, *Google PowerMeter Privacy Policy Notice*, at http://www.google.com/powermeter/privacy.
[72] T.E.D., *Which TED Should I Buy?,* http://www.theenergydetective.com/which-ted.html.
[73] T.E.D., *TED 5000 Which TED*, http://www.theenergydetective.com/which-ted.html (stating that the "CTs are designed to be used to measure the entire home, but they can be used to measure an individual circuit just as well").
[74] T.E.D., *TED 5000 Features*, http://www.theenergydetective.com/ted-5000-features.html.
[75] Earth2tech, *Google PowerMeter Bypasses the Smart Meter*, Oct. 5, 2009, http://earth2tech.com/2009/10/05/googles-powermeter-bypasses-the-smart-meter-signs-up-first-gadget-partner/.

system of customer's house, the number of occupants, and materials used for walls and floors.

Although third-party web portals will have access to, store and use highly revealing customer data, they may not be held to the same confidentiality requirement as the utilities from which the third-party web portals obtains the data, as we will further explain in Section III.B.

The market for Home Area Network (HAN) devices and services is still nascent but rapidly evolving. Some vendors offer consumer-oriented devices such as programmable thermostats and in-home displays,[76] while other vendors provide comprehensive solutions to utilities with HAN as a part of the overall solution.[77] For instance, one vendor, Tendril, has developed a system, called Tendril Residential Energy Ecosystem (TREE) that implements the ZigBee Smart Energy Profile.[78] The TREE system includes data management, data transmission and demand response solutions for utilities, as well as a web portal called Vantage that provides utility customers the tools for HAN registration, device management, consumption data monitoring, etc.[79]

III. Implications of Smart Grid Data Flow for Consumer Privacy

The details of data flow in the Smart Grid, as explored above, provide an important foundation for understanding a range of customer privacy and security issues created by an interconnected digital grid. While the wealth of information collected by Smart Grid technologies provides significant benefits to consumers, it also presents new privacy risks. The unprecedented amount of information collected about customers' energy and appliance use has the potential to reveal intimate details about daily lives and activities inside homes. These risks are compounded by the lack of a clear framework or rules to apply to the new technology landscape, which we discuss below.

A. Customer Data Concerning Home Activities Presents Privacy Risks That Must Be Addressed

Our review in Section II comprises a partial picture of the great variety of information about customers' homes that is or could be collected by various Smart Grid

[76] For example, ZigBee Smart Energy Certified Products include displays, thermostats, and load controllers. See ZigBee Alliance, Zigbee Smart Energy Certified Products, http://www.zigbee.org/Products/CertifiedProducts/ZigBeeSmartEnergy/tabid/271/Default.aspx.

[77] *See* Presentation of Tendril and Landis+Gyr at Texas Smart Energy Forum, http://www.centerpointenergy.com/services/electricity/buildersanddevelopers/smartmeters/d270d7c7a0f33210VgnVCM10000026a10d0aRCRD/.

[78] Tendril, *The Tendril Residential Energy Ecosystem (TREE) Platform Whitepaper*, http://www.tendrilinc.com/wp-content/uploads/tree-whitepaper-v7.pdf.

[79] Tendril, *Put Your Customers in Control*, http://www.tendrilinc.com/utilities/utility-products/products/vantage/. (Note the image on the upper right corner of the webpage.)

technologies and practices. Such information may include device identifiers that uniquely identify a smart device and the manufacturer, control signals that reveal the function of smart devices, energy consumption at frequent time intervals at both the household and device level, temperature inside customers' home, status of smart devices such as IP address and firmware version, and customers' geographic region.

In addition, with the rapid development of analytical software, consumption data, either taken by itself or combined with other information, may be used to infer even more details about customers' lives inside their homes. For instance, even if energy consumption is not collected for individual appliances, information about energy consumption of individual appliances can be reconstructed from aggregate smart meter reading data of a household by using non-intrusive appliance load monitoring ("NALM") techniques.[80] Researchers can compile libraries of appliance load patterns and match similar patterns in the time series data of overall utility usage records.[81] Research shows that analyzing fifteen-minute interval aggregate household energy consumption data can by itself pinpoint the use of most major home appliances.[82] As the time intervals between data collection points decreases, home appliance use will be inferable from overall utility usage data with greater and greater accuracy.

The great variety of information about customers' homes being collected or likely to be collected, as well as analysis of that information, gives rise to serious privacy concerns. Home appliance use reflects intimate details of people's lives and their habits and preferences inside their homes. As Justice Scalia recognized in *Kyllo v. United States, "*at what hour each night the lady of the house takes her daily sauna and bath" is "a detail that many would consider 'intimate.'"[83] Some of the activities that might be revealed through the Smart Grid 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, or simply unorthodox, behavior.[84] As a result, information collected by the Smart Grid is valuable for many purposes other than energy efficiency, most prominently commercial exploitation by advertisers and marketers, access by criminals who wish to peek into homes, and access to household information and surveillance by law enforcement, as discussed further below.

In identifying standards and making recommendations for technology design and service deployment, NIST should consider what uses of this information may emerge that could have an adverse impact on consumers, invading the traditionally protected zone of

---

[80] Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies*, May 9, 2009, http://ssrn.com/abstract=1462285, at A-1.
[81] *Id*. at 2. The construction of load pattern libraries can be manually crafted, or generated by machine learning algorithms such as a neutral network.
[82] 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, http://ssrn.com/abstract=1370731, at 28.
[83] *Kyllo v. United States*, 533 U.S. 27, 38 (2001).
[84] 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.

the home and home life. Without planning, such adverse impacts could drive opposition to the Smart Grid and prompt a backlash against data collection that could be socially beneficial when limited to the narrow purposes of improving efficiency. For example, much of the information collected by the Smart Grid about customers is commercially valuable, and could be resold for a profit. In other contexts, companies have repurposed information in ways that are beyond the bounds of consumer bargaining or expectations.[85]

Because of the intimacy of home life, data collected by Smart Grid technologies and services could be put to especially trangressive purposes. For example, an analysis of smart meter data revealing customers' home activities and daily routines could be commercially valuable to life insurance companies looking to adjust rates for customers with purportedly unhealthy lifestyles. Financial institutions making home mortgage loans might also be interested in their customers' energy usage records to verify whether the customers are actually living in those houses. Advertising companies offering behavioral targeting products might wish to enhance existing customer profiles with energy usage data revealing customer activities and habits, following a recent trend in the merging of online and offline data sources to support more targeted third-party advertising.[86] As explained in Section II, device identifiers and control signals reveal to the utilities the manufacturers, functionality, and usage of smart devices, which is valuable for the market research and marketing efforts of smart appliances manufacturers and others who wish to target particular demographic groups. Data brokers, advertisers, marketing research firms, and others might also find this type of detailed information about customer habits attractive.

Criminals might also seek access to smart meter reading data or other information collected by the Smart Grid, in hopes of using 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 and other revealing information over long periods of time, information-gathering via Smart Grid technologies could reveal behavior patterns likely to be repeated in the future, allowing criminals to plan for future attacks. If 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, especially when utilities or other providers use unsecured paths to transmit data. For instance, many businesses and others traditionally use energy

[85] There are many examples of this phenomenon, but recent examples include employers and insurance companies using information posted on social networking services to screen employees and to deny insurance claims. *See* Michal Czerwonka, *Facebook Page Costs Woman Her Benefits*, Wall St. Journal, Nov. 24, 2009, http://online.wsj.com/article/SB10001424052748704779704574554380064654604.html; BNA Privacy & Security Law Report, *Employment Issues: Court OKs Verdict Against Restaurant For Managers' Access of MySpace Account*, 8 PVLR 1474.

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

consumption data to authenticate customers, making the information particularly valuable to those attempting illicitly to take over someone else's account.[87] Threats to customer data security are compounded if the data transmission within Smart Grid networks is not encrypted, in which case criminals may be able to easily intercept Smart Grid transmissions and acquire the content of communications.

For a variety of reasons, law enforcement officials may also be interested in the fine-grained data about household habits collected by the Smart Grid. As part of their investigatory work to solve crimes, officials may want to establish or confirm 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 indicates illegal or other 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.[88] The data from Smart Grid technologies certainly may be highly useful for these purposes. At the same time, the privacy implications of law enforcement officials' interest in obtaining smart meter data suggest the need for strong Fourth Amendment procedural protections for this information, as well as careful procedures on the part of utilities and other providers, and technology design that allows for strong data protection. Already, a California family was put under surveillance by law enforcement for having an unusually high electricity bill, which turned out to merely reflect the legitimate activities of a busy household.[89] Procedural safeguards may be especially important in light of the fact that 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.[90]

B. Longstanding Special Protections for Information about the Home and Home Life, Combined with the Lack of Clear, Consistent Rules for the Smart Grid, Highlight Privacy Risks and Create a Strong Need for Privacy Protections to Be Included in Technological Design and Service Provider Practices

Under longstanding U.S. constitutional values and law, activities occurring within the sanctity of individuals' homes, because of their inherently personal nature, have been

---

[87] 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.

[88] 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, http://groups.ischool.berkeley.edu/samuelsonclinic/files/demand_response_CEC.pdf (under 3.2.4, Law Enforcement Practices) (hereinafter "Berkeley/CyberKnowledge Report").

[89] Channel10 San Diego News, *High Electric Bill Leads To Calif. Police Raid*, March 28, 2004.

[90] *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.

afforded special protection from intrusion by others.[91] 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."[92] 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.[93] Data collected via Smart Grid technologies are similarly revealing of the intimate details of home life, and should be subject to similarly high levels of protection.

At the same time, the customer data collected and used in the Smart Grid is governed by a patchwork of broad state and federal laws that may be generally applicable, but those often 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 customer privacy law in the U.S. that might generally cover commercial activities related to Smart Grid information.

We appreciate NIST's recognition that a "lack of consistent and comprehensive privacy 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."[94] 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.[95] 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. As such, technology design and utility and third-party service provider practices must be carefully considered and rigorously implemented in order to protect customer privacy and security.

Historically, the principal source of privacy regulation for electricity data has been state public utility commissions, which place varying restrictions on consumer energy data. [96] In some states, utilities may provide competitive suppliers access to

---

[91] *Id*.
[92] *Kyllo v. United States*, 533 U.S. 27, 37 (2001).
[93] *Id*. at 40.
[94] 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 84.
[95] Berkeley/CyberKnowledge Report at 23.
[96] Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies*, May 9, 2009, http://ssrn.com/abstract=1462285, at 24.

customer energy data without the ratepayer's affirmative consent.[97] While other 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 some types of Smart Grid data.[98] And generally, state utility commissions are just beginning to consider the privacy implications of Smart Grid data.[99] General state laws governing business' and third parties' collection and use of customers' personal data may apply to energy usage, but may be too narrow to cover the extensive and varied information generated by the Smart Grid, or the increasing number of entities that have access to the information. For example, California Public Utility Code §394.4 imposes a general requirement on electric service providers to ensure confidentiality of customer information,[100] However, the emergence of third-party service providers such as Google PowerMeter and Microsoft Hohm means that new entities have access to customers' private data, but likely stand outside the statutory confidentiality requirement because they are not "electric service providers" under California law.[101] Furthermore, new types of information, such as the unique identifiers of smart devices collected by the utilities, create uncertainties about whether current privacy law could be extended to these new types of information.[102] It is also important to note that California has a relatively protective regime for personal data and other states' privacy regulations may vary greatly in terms of the rules governing utilities and third party service providers.[103]

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, one of the greatest privacy concerns for consumers is

---

[97] Before the Federal Communications Commission in the Matter of International Comparison and Consumer Survey Requirements in the Broadband Data Improvement Act, *Comments of the Edison Electric Institute*, GN Docket No. 09-47, Oct. 2, 2009, at 28.

[98] *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.

[99] For example, the National Association of Regulatory Utility Commissioners (NARUC) will consider a resolution in 2010 that would encourage member states to support several regulatory protections on consumer data collected in the Smart Grid. *Draft Resolutions Proposed for Consideration at the 2009 Annual Convention of NARUC*, submitted Nov. 5, 2009, http://annual.narucmeetings.org/09_1106_Proposed_Resolutions.pdf, at 14-17. *See also* 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 84.

[100] California Public Utility Code §394.4 ("Confidentiality: Customer information shall be confidential unless the customer consents in writing. This shall encompass confidentiality of customer specific billing, credit, or usage information").

[101] For a list of electric service providers registered with the California Public Utilities Commission, see http://docs.cpuc.ca.gov/published/ESP_Lists/esp_udc.htm.

[102] For example, California Penal Code §1326.1.(a) requires that law enforcement should show specific and articulable facts before accessing "utility records," which includes billing and payment information but may or may not include customers' device identifiers under California law.

[103] *See* Andrew B. Serwin, *Information Security and Privacy: A Practical Guide to Federal, State and International Law*, § 28:28 – 44 (2009) (providing an outline of California privacy protections).

what the utilities will do with information they receive from their customers, and ECPA places no limit on that. The FCC's Customer Proprietary Network Information (CPNI) Rules, which require telecommunications carriers to obtain customers' opt-in before using, disclosing, or permitting access to individually identifiable customer information, do not necessarily directly bear on the privacy issues surrounding a Smart Grid information network.[104] 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.[105] 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 customer's home computing system might generate liability under an expansive reading of the CFAA.[106] 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.[107]

This brief and introductory discussion of the rules possibly applicable to Smart Grid technologies reveals the disjointed and outdated nature of current customer protections for energy data. Industry lacks a clear set of privacy guidelines to govern Smart Grid technologies. In light of the legal patchwork, we are especially in need of a cohesive approach that reflects the realities of an interconnected and digitized electricity grid in which customers are active contributors of personal data. As further explored below, we encourage NIST to include in its Framework comprehensive privacy principles against which technical standards can be evaluated to ensure that both Smart Grid technologies and service providers are sufficiently protective of consumer privacy.

IV. Proposed Framework for NIST Privacy Principles

The discussion of unique risks to privacy presented by the Smart Grid, and the present lack of comprehensive legal rules mitigating those risks, reveals the need to develop strong design and business practice mechanisms for protecting consumer privacy in the modernized grid. In the following section, we lay out the necessary elements for developing a comprehensive framework to protect privacy in the Smart Grid, including who should be covered, what types of data should be included, and how principles can

---

[104] Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies*, May 9, 2009, http://ssrn.com/abstract=1462285, at 25-26.
[105] Mark Foley, *Data Privacy and Security Issues for Advanced Metering Systems,* SmartGridNews.com, July 1, 2008.
[106] 18 U.S.C. § 1030; *See also* Berkeley/CyberKnowledge Report at 28.
[107] *See* Mark Foley, *Data Privacy and Security Issues for Advanced Metering Systems*, SmartGridNews.com, July 1, 2008.

ensure the fullest protections for consumers' Household Energy Data. All of the technical standards identified by NIST for implementation in the Smart Grid should be evaluated against these principles, and ultimately, the Framework for standards and requirements released by NIST should reflect these principles.

A. Privacy Principles Should Cover All Smart Grid Entities and Practices

Ensuring that the full range of companies touching consumer data in the Smart Grid are covered by any privacy protections is critically important. In the current NIST Draft, the examination of privacy risks and potential safeguards in Chapter Two focuses too narrowly on "consumer-to-utility" data flows.[108] Instead, the activities of utility companies, third party service providers, such as Microsoft and Google, and device manufacturers, such as General Electric and Honeywell, in collecting, using, and storing consumer data should all be considered, and technical standards should be evaluated in light of known business practices and service models in addition to technology capabilities. Privacy principles should not subject different entities to a different set of rules where the entities are similarly interacting with consumer data. Furthermore, recognizing this universe of participants now is important in fully incorporating "privacy by design" into the applicable standards and technologies underlying the Smart Grid.

In performing an evaluation of the proposed standards, a well-developed set of use cases explaining how privacy principles should be built into the Smart Grid will be important in ensuring the full implementation of consumer privacy protections. For the final Framework, NIST should develop use cases that reflect a comprehensive model of data flow, covering all entities and activities, and detail the necessary consumer privacy protections which should be required in all Smart Grid standards and technical requirements.

B. Privacy Principles Should Cover "Household Energy Data"

Designing an effective framework to protect consumer data also requires specific consideration of what information requires protection. As drafted, the privacy principles in the NIST Draft are built upon the model of "personally identifiable information" ("PII"), including the "notice and purpose for PII use," "collection of PII," and the "use and retention of PII."[109] In the context of the Smart Grid, however, the privacy assessment of consumer data practices must extend beyond traditional notions of PII, which has a longstanding history of special legal consideration for its ability to directly identify an individual, such as a name, address, email address, or phone number. Certainly some of the data collected by utilities and third party service providers in the Smart Grid, such as name and address for billing purposes, would be considered PII

[108] NIST, *Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy and Requirements*, at 8.
[109] *Id*. at 12.

under traditional definitions. But based on the discussion of consumer data flow described above in Section II, it is clear that some data collected and used in the Smart Grid extends beyond traditional PII, yet is very revealing of traditionally protected household activities and intimate home life.

As such, we recommend that NIST adopt privacy principles that cover a somewhat broader set of intimate information: "**Household Energy Data**." Household Energy Data includes: any consumption or device data capable of revealing personal or household information that is not aggregated over long periods of time or over a large number of ratepayers.[110] Specifically, Household Energy Data includes both:

(a) traditional PII, such as account information used for billing purposes and unique device identifiers tied to an individual name, which is either immediately personally identifiable or becomes personally identifiable when combined with other collected information; and

(b) data collected about an individual household in the Smart Grid that is revealing of home life by itself or when analyzed or combined with other information. Examples of this second category of Household Energy Data include: near real-time energy usage data, records of plug-in hybrid electric vehicle (PHEV) use, and specific metering data (e.g. thermostat temperature).

Sometimes information in the second category will be personally identifiable when combined with other types of information, or when the number of people in a household is small, while sometimes it is unlikely to identify individual members of a household, at all. Regardless of whether it is identifiable, however, it is inherently revealing of household activities and home life, traditionally private domains that are, and should continue to be, protected from observation. While not all Household Energy Data may uniquely identify an individual in a multi-person household, it can still reveal highly personal and invasive details about daily activities of people living in the home, such as the use of a specific medical device or an absence from the home, raising the serious privacy issues explored above. Further, given that 32.2 million people live alone in the U.S and twenty eight percent of American households have single-person occupancy,[111] Household Energy Data is revealing of individual activity for a significant number of Americans.

Examples of data not covered by "Household Energy Data" include usage records aggregated in 30-day increments—what is collected now through monthly metering readings—and other types of data aggregated across a large number of

[110] Utilities may generally refer to information of this type as "customer usage information," which may also be an appropriate term provided it includes the elements detailed above. *See* utilities' comments in a recent CPUC rulemaking, California Public Utility Commission, Proposed Decision of Commissioner Chong, Agenda ID #9052, Nov. 17, 2009, http://docs.cpuc.ca.gov/efile/PD/109890.pdf.

[111] U.S. Census Bureau, *Facts for Features: Unmarried and Single Americans Week*, July 21, 2009, http://www.census.gov/Press-Release/www/releases/archives/facts_for_features_special_editions/014004.html.

households. While still needing some safeguards, such data likely does not require the full scope of protections outlined here.

We also note that this working definition of Household Energy Data, and the following discussion of a privacy framework to protect this data, is intended to be a baseline for the least revealing information included within the definition. Some of the information included within the set of "Household Energy Data," such as PII and location-identifying information will likely require additional protections. The principles discussed here for Household Energy Data outline the minimum protections required for this basic category of data.

C. Privacy Principles for Household Energy Data Should be Grounded in Comprehensive Fair Information Practice Principles (FIPPs)

Here, we consider the larger question of how to protect the Household Energy Data collected and used in the Smart Grid. Properly formulated and rigorously implemented **Fair Information Practice Principles ("FIPPs"**) provide a broad, comprehensive privacy framework that should underlie privacy standards for the Smart Grid. We urge NIST to adopt appropriately formulated FIPPs as the basis for its consumer privacy recommendations. While we appreciate the Cyber Security Coordination Task Group's (CSCTG) effort to consider a set of rules extending beyond notice and consent, the privacy principles as drafted need considerably more specificity and organization. Given the broad acceptance of FIPPs by national and international privacy regulators, the fact that they have been applied in many contexts related to consumer privacy, and the fact that the lesser-known Generally Accepted Privacy Principles (GAPP) cited in the NIST Draft are grounded in FIPPs, it is most sensible to revise the Draft's privacy principles to more fully reflect FIPPs.

In particular, the technical standards and requirements ultimately recommended by NIST should incorporate FIPPs, and should recommend that relevant technologies be designed to have the capacity to implement FIPPs, and to interoperate based upon them, enabling "privacy by design." While various versions of FIPPs are used by different regulatory bodies, we consider here, and recommend for adoption, the articulation of FIPPs in the Department of Homeland Security's (DHS) 2008 Privacy Policy memorandum. Compared to prior versions of FIPPs, that sometimes provided vague, incomplete, and generally weakened privacy protections,[112] the DHS framework is the U.S.-based framework that most closely follows strong international interpretations of FIPPs. It provides a robust set of modernized principles that NIST should apply to all entities collecting consumer data in the Smart Grid. These principles include:

[112] For an expansion of this critique, see CDT, *Refocusing the FTC's Role in Privacy Protection: Comments of the Center for Democracy & Technology In regards to the FTC Consumer Privacy Roundtable*, Nov. 6, 2009, http://www.cdt.org/privacy/20091105_ftc_priv_comments.pdf, at 6-7.

1. **Transparency**: Smart Grid entities should be transparent and should provide meaningful, clear, full notice to the individual regarding the collection, use, dissemination, and maintenance of Household Energy Data.

Relevant information about the collection, use, dissemination and maintenance of Household Energy Data must be shared with the consumer. This information-sharing must extend beyond mere notice of collection practices; it must also include providing consumers with clear, detailed information about the specific uses of their data, retention periods, and any transfers of data to or access by other entities. Notices should state clearly: what information is collected, whether this information is shared and with whom it is shared, the period that data is retained, and the contact information for an official at each company responsible for the policy and for personal data collected by the system. For example, device manufacturers should clearly provide notice of any transfer of data, such as device status being transmitted from the device to the manufacturer, which might occur with the consumer's use of a device. Further, Smart Grid entities, including utilities, third-party service providers, and device manufacturers, should also provide consumers with access to the personally identifying information collected about them, as well as Household Energy Data collected about their homes.

2. **Individual Participation**: Entities should involve the individual in the process when using energy information and, to the extent practicable, seek ratepayer consent for the collection, use, dissemination, and maintenance of Household Energy Data. Entities should also provide mechanisms for appropriate access, correction, and redress regarding their use of Household Energy Data.

The NIST draft recognizes that "new smart meters create the need for utilities to give residents a choice about the types of data *collected*,"[113] but consumer choice must also extend to the *use, transfer, and maintenance, including retention,* of Household Energy Data. To fully recognize the principle of individual participation, Smart Grid entities must respect the range of consumer preferences with respect to their data that will exist at multiple points along the data path.

Initially, consumers should be required to opt in to the collection and use of Household Energy Data for any secondary purposes beyond what is strictly required for the provision of service. Without affirmative consent by the consumer, any use of data by utilities or third party service providers should be limited to purposes related to the original mission of the service or application. The opt-in consent should allow the consumer to exercise a genuine choice, meaning that it does not present high practical barriers or costs if the consumer chooses not to opt in.

In the case of utilities, this means that opt-in consent would be required for a utility to use Household Energy Data for delivering advertisements to its customers, which is clearly unrelated to the primary purpose of providing energy service. A third

[113] NIST, *NIST Draft NIST Interagency Report (NISTIR) 7628*, at 12 (emphasis added).

party service provider's use of device identifiers for marketing purposes is another example of using data for a secondary purpose. As explored further in the Use Limitation principle, NIST should develop use cases that provide specific guidance on what constitutes acceptable primary and secondary purposes of data use in the Smart Grid.

Informed consumer consent should also be affirmatively required for any access to or transfer of Household Energy Data to or by third party service providers. At all points, consumers should have reasonable access to the Household Energy Data that utilities or third-party service providers are collecting and using, with mechanisms available to correct data where it contains inaccuracies and to actively manage secondary uses. There should also be parity in enrollment and any opt-out/opt-in mechanisms. That is, if an individual or household can enroll in data sharing online, they should also be able to cancel that sharing and exercise other choices about their data through the online mechanism.

3. **Purpose Specification**: Companies should specifically articulate the purpose or purposes for which Household Energy Data will be used.

The specification of purpose should fully describe both primary purposes of data use by the utility or service provider, and any secondary purposes, as described above. Consumers should be provided with this information about how their data will be used *before* the time of collection by service providers. The NIST Draft allows for disclosure "at the time of collection,"[114] but that may not provide consumers with the necessary opportunity for individual participation, which includes sufficient opportunity to separately opt in to any use of their Household Energy Data for secondary purposes.

Clearly articulating the purpose of data use enables the consumer to make an informed choice before deciding to share data. In the context of the Smart Grid, for example, one would expect a utility to specify to a consumer that "Household Energy Data" will be used for the primary purposes of providing time-of-use pricing that may reflect discounted rates during certain times of the day. A third-party service provider offering consumers an online interface for monitoring energy consumption may specify that Household Energy Data will be used to target product advertisements to the consumers (which, again, is likely the use of consumer data for a secondary purpose, requiring affirmative, additional consent). If the utility later changes the purpose for which the Household Energy Data is used, consumers should also opt in to that new use.

4. **Data Minimization**: Only data directly relevant and necessary to accomplish a specified purpose should be collected and data should only be retained for as long as necessary to fulfill the specified purpose.

Generally, Smart Grid technical standards should support, and technologies

[114] NIST, *NIST Draft NIST Interagency Report (NISTIR) 7628*, at 12.

should be capable of, appropriate data minimization. In the context of the utility, the Data Minimization principle means that utilities' collection of data for the primary purpose of providing energy use should be limited to that information necessary for billing, load management and some demand response programs—information that is "directly relevant and necessary" to the provision of the primary service. As the NIST Draft importantly notes, "only the minimum amount of data necessary for utility companies to use for energy management and billing should be collected."[115] Further explanation of the specific types of information necessary for utilities to perform these functions in a data minimizing manner should be detailed in the set of use cases developed by NIST, as suggested above. At the outset, we note that it is unlikely the utilities need to collect information about the functioning of individual appliances, or even individual houses, to implement load management or demand response programs.

Centralizing the collection and usage of Household Energy Data at the Smart Meter level would also enable such minimization. As smart meters become capable of more sophisticated computation, they should be engineered so that it is possible to aggregate the collection, use, and storage of private data at the point of consumption. Such a meter would aggregate and anonymize usage records over both time sequence and type of appliance so as to report only relevant abstractions of data such to the utility. It would also enable consumers to have their smart devices communicate securely with the HAN or other gateway without revealing the details of their smart devices, or the time of use, to the utility.[116] Designing smart meters and other devices to preserve privacy by default enables households to fully participate in the decision to share their Household Energy Data outside of the home. Minimizing the data that leaves the home is especially important because of the well-established constitutional protections for data residing in the home, as discussed earlier.

While there are some likely consumer advantages tied to sending Household Energy Data to the utility (e.g. a utility may offer price discounts for consumers who share data beneficial for load research), our initial research suggests that the efficiency benefits of the Smart Grid can be realized without centralizing all control of Household Energy Data at the utility. Existing meters should be updated where possible within technological constraints, and new meters should be designed, so that consumers can choose to minimize the sharing of Household Energy Data with utilities or third-party service providers. Meters with sufficient processing and storage capacity to manage demand response pricing within the home are not currently being widely marketed, but advanced smart meters such as Itron's OpenWay CENTRON meter, which has the capability for performing complex usage calculations and storing large quantities of data, already reveal that smart meters can allow for data minimization while still enabling the

[115] NIST, *NIST Draft NIST Interagency Report (NISTIR) 7628*, at 12.

[116] Note that in the ZigBee Smart Energy Profile, customers must reveal details of their smart device to utilities in order to register and authenticate their smart devices with a home area network. An alternative design may not require so much detail about customers' smart devices in its implementation of the same function.

benefits of the Smart Grid. Where Smart Meters are already being installed without any capability for data minimization,[117] NIST should adopt technical recommendations that provide for this option, especially since devices already in the field can be updated remotely.

Applying the data minimization principle to utilities also means that current retention periods for customer records, which currently widely reflect the industry standard of seven years,[118] should be revised in light of the Smart Grid transition and attendant collection of Household Energy Data. Beyond the security advantages of reducing retention, shorter periods will likely yield benefits to the utilities in terms of decreased storage and maintenance costs.[119]

Applying this principle to third party services providing consumers with web-based visual representations of home energy use, such as MS Hohm, suggests that those service providers should not collect appliance-level device identifiers (unless a purpose such as consumer marketing was specified to the consumer and opt-in consent was obtained prior to the use, per the principle above). Third party service providers should also enable consumers with the choice to end service and terminate their accounts, including the prompt deletion of any Household Energy Data retained by the utility.

5. **Use Limitation**: Household Energy Data should be used solely for the purposes specified in the notice. Sharing of such information should be only for a purpose compatible with the purpose for which it was collected.

In the case of a utility collecting Household Energy Data for the primary purpose of providing energy service to the ratepayer, access to that data should be limited within the utility to entities with a justifiable requirement to use the data for fulfilling the clearly-specified purpose, such as the billing department. Any secondary uses beyond those must be specified in advance, and should only occur with explicit consumer consent under an opt-in regime, as detailed above. For example, detailed information about a consumer's smart devices, such as a MAC address uniquely identifying the device and the manufacturer of the device, should not be used by a utility or third party service provider, unless such use was specified to the consumer, who specifically opted in to the purpose. Similarly, third party service providers should not use Household Energy Data

[117] Utilities have already begun to deploy Smart Meters to customers. In Northern California, PG&E's Smart Meter implementation has generated controversy among customers complaining of higher bills and prompted a class-action suit. *See* Andrew Koskey, *Smart Meters Come Under Fire*, San Francisco Examiner, Nov. 26, 2009, http://www.sfexaminer.com/local/Smart-meters-come-under-fire-73831897.html.
[118] Berkeley/CyberKnowledge Report.
[119] Robert Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete* (2002), http://epic.org/reports/dmfprivacy.html.

for behavioral advertising or other marketing purposes when the primary purpose of the data collection and use specified to the user was more limited.

6. **Data Quality and Integrity**: Companies should, to the extent practicable, ensure that data is accurate, relevant, timely and complete. Utilities and other entities handling Household Energy Data, including third-party service providers, should provide consumers with tools to correct mistakes or challenge information provided in profiles.

The NIST Draft importantly noted this need to allow consumers to review and correct, where necessary, their information. Standards and technical requirements implemented by utilities and third party service providers, for example, should allow for easily-accessible interfaces which give consumers the opportunity to review and correct their Household Energy Data. This review provides the best means of ensuring that consumer data is accurate, which is particularly important given companies' data retention and transfer practices.

7. **Security**: Companies must protect Household Energy Data through appropriate security safeguards against risks of loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure, and Smart Grid technologies and services must be capable of implementing these security safeguards. Reasonable security in the Smart Grid requires that any transmission of Household Energy Data must be secure and that data practices by utilities and other providers include meaningful safeguards for Household Energy Data.

For example, if a communication is sent over an open wireless connection, or could otherwise be intercepted with reasonable or targeted efforts, encryption should be required, for both organization-owned infrastructure and third-party communication services. More broadly, technical standards identified by NIST for implementation should be reviewed and, if necessary, revised to require that smart-device communications provided by either utilities or third-party service providers are truly secure, prior to any recommendations being made. For example, contrary to the Draft's requirement that "[d]emand response HAN devices must be securely authenticated to the HAN gateway and vice versa,"[120] both OpenHAN and ZigBee standards presently identified as NIST standards for implementation include scenarios (in the provided background context for relevant use cases) in which smart devices respond to open radio signals to provide demand response capabilities.[121] NIST should recommend that these standards be revised, as unauthenticated HAN devices responding to open, unencrypted signals pose a clear security risk for consumers.

[120] NIST, *NIST Draft NIST Interagency Report (NISTIR) 7628*, at Appendix D, D.10.
[121] *See* UtilityAMI, *OpenHAN System Requirements Specification*, at 27; ZigBee Alliance*, ZigBee Smart Energy Profile Specification*, at 189.

Further, Household Energy Data collected, used and maintained by utilities or other service providers must be stored securely, and must be maintained subject to secure data management practices. If a security or other breach results in the loss or exposure of Household Energy Data, affected customers should be notified and all reasonable steps should be taken to minimize harm to customers.

8. **Accountability and Auditing**: Companies should be accountable for complying with these principles, should provide appropriate training to all employees and contractors who use Household Energy Data and should audit the actual use of that information to demonstrate compliance with the principles and all applicable privacy protection requirements.

NIST's current draft recognizes the importance of this principle in stating that "documented requirements for regular privacy training and ongoing awareness activities for all utilities, vendors, and other entities with management responsibilities throughout the Smart Grid should be created and implemented, and compliance enforced."[122] As discussed above, an important means of ensuring widespread implementation of the full set of FIPPs is to develop rigorous, comprehensive use cases that reflect a comprehensive model of data flow as well as these principles, and that inform the development of specific privacy requirements against which companies can audit for compliance purposes. In expanding the next iteration of the Draft, and specifically in further developing the Privacy chapter, the CSCTG should develop or collect these use cases.

The CSCTG should also consider outlining an accountability mechanism, such as a certification programs for Smart Grid technologies and third-party services, to measure adherence to privacy principles grounded in FIPPs. Such a certification program could be helpful in establishing an industry standard for data practices by utilities or other providers that provides meaningful safeguards for the Household Energy Data. In developing such a program, California's experience in certifying meters could be instructive.[123]

V. General Recommendations

As the exemplified in the prior discussion, crafting a comprehensive privacy framework for the Smart Grid is a complex task requiring the careful examination of

---

[122] NIST, *NIST Draft NIST Interagency Report (NISTIR) 7628*, at 12.

[123] California adopted permanent standards for meters in California Public Utility Commission (CPUC) Decision No. 98-12-080, http://www.cpuc.ca.gov/PUC/energy/Retail+Electric+Markets+and+Finance/Electric+Markets/Metering/msp_info.htm, http://www.cpuc.ca.gov/PUC/energy/Retail+Electric+Markets+and+Finance/Electric+Markets/Metering/mp_process.htm. Meter manufacturers could "self-certify" their meter products by submitting a self-certification form to CPUC, stating that the meter meets the standards for certification, subject to the review and approval of CPUC.

rapidly evolving technology and business models. While well-developed tools, such as the robust articulation of FIPPs outlined here, can be quite helpful in creating privacy principles for the Smart Grid, more work must be done to apply these guidelines to modernized Grid technologies and specifically to the full set of NIST recommended standards and technical requirements that will emerge from the standards-setting process. As a priority for future work, we recommend that the CSCTG devote energy to developing a specific set of uses cases that reflect a comprehensive model of consumer data flow related to Smart Grid technologies and services and that are informed by the FIPPs-based framework set forth above. In addition to helping companies in the auditing process, as described above, developing a rigorous set of uses cases now will provide an important mechanism for identifying further changes that need to be made to the proposed standards to protect consumer privacy, and for evaluating where additional standards may need to be created.

Finally, fully addressing the implications of utilities and third-party application providers' greatly enhanced collection and use of Household Energy Data in the Smart Grid may require more time than has been allocated in the current process. While we understand the tremendous interest in accelerating the deployment of Smart Grid technologies, we also strongly support NIST's observation in the Framework and Roadmap, 1.0 that the development process "must be systematic, not ad hoc."[124] While it is certainly true that "[l]egal and regulatory frameworks can be further harmonized and updated as the Smart Grid becomes more pervasive,"[125] it is critical to develop a full, carefully considered privacy assessment now, so that the applicable standards are crafted in a way that protects consumer privacy. We suggest that the timeline for CSCTG's work be considered, and readjusted if needed, to ensure there is sufficient opportunity for a full review of these issues, including the development of the privacy use cases described above. This may require that NIST extend the target date for the completion of the final Draft.

VI. Conclusion

We greatly appreciate NIST's attention to consumer privacy in the Smart Grid, and encourage the prioritization of these important issues in further work to finalize the Cyber Security Strategy and Requirements document and Framework. As noted earlier, we are at a critical point in the deployment of new Smart Grid technologies, necessitating immediate attention to consumer privacy and security risks. Failure to ensure adequate consumer protections in NIST's recommended standards and technical requirements for the Smart Grid could encourage the development of technologies and services that do not adequately protect privacy within the intimate realm of the home, undermining consumer confidence in these promising new technologies. By adopting robust privacy principles

[124] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, Sept. 2009, at 22.
[125] *Id.* at 84.

that recognize the sensitive nature of Household Energy Data and ensuring the implementation of these principles in its technical standards, NIST can provide much-needed guidance to the energy community about how best to safeguard consumers while still realizing the promise of the Smart Grid.

We look forward to providing any further information that may be useful.

Respectfully submitted,

Jennifer M. Urban
Elizabeth Eraker
Longhao Wang

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

on behalf of the Center for Democracy & Technology

December 1, 2009