UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF ENERGY

Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use and Privacy	))))	Request for Information

---

COMMENTS
BY
THE NATIONAL ASSOCIATION OF STATE UTILITY CONSUMER ADVOCATES

NATIONAL ASSOCIATION OF STATE UTILITY CONSUMER ADVOCATES
8380 Colesville Road, Suite 101
Silver Spring, MD 20910
Phone (301) 589-6313
Fax (301) 589-6380

July 12, 2010

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF ENERGY

Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use and Privacy	))))	Request for Information

---

COMMENTS
BY
THE NATIONAL ASSOCIATION OF STATE UTILITY CONSUMER ADVOCATES

The National Association of State Utility Consumer Advocates ("NASUCA") hereby submits the following comments in response to the United States Department of Energy ("DOE") Request for Information ("RFI") entitled "Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy." See 75 Fed. Reg. 26203 (May 11, 2010).[1] The RFI requests comments and information from interested parties to assist DOE in understanding current and potential practices and policies for the states and other entities to empower consumers, and perhaps others, through access to detailed energy information in electronic form—including real-time information from smart meters, historical consumption data, and pricing and billing information.

NASUCA is a voluntary organization comprised of offices from 40 states and the District of Columbia, charged by their respective state laws to represent utility consumers before federal and state utility regulatory commissions, before other federal and state agencies, and before federal and state courts. Many NASUCA members have extensive experience with regulatory policies governing the utility industry and have participated in proceedings concerning smart grid

[1]NASUCA is also submitting separate comments in response to the DOE RFI entitled "Implementing the National Broadband Plan by Studying the Communications Requirements of Electric Utilities to Inform Federal Smart Grid Policy." See 75 Fed. Reg. 26206 (May 11, 2010).

and consumer privacy issues. NASUCA members' primary interest is the protection of residential and other small utility consumers' interests.

DOE's RFI seeks to collect information and open a dialogue about the challenges inherent in empowering consumers, utilities, and third parties to realize the many potential benefits of the smart grid, meeting consumer expectations of privacy and security ease-of-access, and providing the flexibility to manage all of them. NASUCA's Comments will address the list of questions included in DOE's RFI in order to help DOE identify policies and practices that will effectively take into account the interests of consumers, including the retail residential consumer class.

INTRODUCTION

The smart grid and additional advancements in technology may allow more products to connect to the grid, thereby expanding the types and amount of data that can be collected and accessed. The personal energy usage information data available from smart grid technologies may potentially expose almost endless amounts of private consumer information, including, but not limited to, personal billing information, when individuals are home, what appliances they use, how long and how frequently they use those appliances, when they take vacations, what their socio-economic status is, whether they observe particular religious holidays, what types of food they eat for dinner, and when they are most likely to alter daily routines.

The personal customer information accessibility enabled by smart grid may appeal to many parties for a variety of uses. Entities that may seek personal customer information include: energy companies seeking to improve service or sell information for profit, third-party marketers, law enforcement agencies investigating possible criminal acts, insurance companies

seeking to identify unhealthy behaviors in order to adjust rates, criminals attempting to perpetrate illegal acts, researchers looking to create new energy-related studies, and competing businesses or manufacturers wishing to access trade secrets of competitors.[2] While offering potential energy management benefits by empowering consumers with information, the interconnectedness of the smart grid makes data carried over the communications networks vulnerable to improper access by unauthorized persons as well.

The advanced metering infrastructure will at a minimum capture and store data on all consumers' hourly usage. This information could be used to estimate which customers have which types of appliances and equipment at home. It could be used to estimate whether a customer is home, weekdays, or for several weeks during vacation. If customers install Home Area Networks ("HAN") and tie their appliances and computer in to the network, that network could be hacked, and specific information about electricity usage could be obtained. To the extent all these systems are hooked into the customer's internet connection, the customer's computers could be at risk, as well.

In the draft Roadmap released September 24, 2009, the National Institute of Standards and Technology (NIST) noted that the major benefit provided by the smart grid, the ability to get richer data to and from customer meters and other electric devices, "is also its Achilles' heel from a privacy viewpoint."[3] NIST went on to say that privacy advocates have raised serious concerns about the type and amount of billing and usage information flowing through the various components of the smart grid, information "…that could provide a detailed time-line of activities occurring inside the home."

---

[2]For a more in-depth look at grid security, *see* NIST Framework and Roadmap for *Smart Grid Interoperability Standards, Release 1.0,,* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Available at* http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf ("NIST Roadmap").

[3]NIST Roadmap at 84.

In a NIST draft report on Smart Grid Cyber Security Strategy and Requirements,[4] the authors stated that a major problem facing the smart grid today is the lack of coordination among different government jurisdictions with responsibility for protecting consumer privacy:

> Most states have general laws in place regarding privacy protections. However, these laws are most often not specific to the electric utility industry. Furthermore, enforcement of state privacy related laws is often delegated to agencies other than public utility commissions, who have regulatory responsibility for electric utilities. Research indicates that, in general, state utility commissions currently lack formal privacy policies or standards related to the Smart Grid. Some individual utility implementations of the Smart Grid are currently at an early stage, while others are more fully developed. Utilities at an early stage of implementation may have not yet documented or implemented privacy policies, standards, or procedures for the data collected throughout the Smart Grid. Comprehensive and consistent definitions of personally identifiable information ("PII") do not typically exist at state utility commissions, at FERC, or within the utility industry. The 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.[5]

State utility regulations typically provide the most significant oversight of energy data access by non-governmental third parties.[6] These regulations may dictate what information belongs to customers and what information must be protected by energy companies. Under some state regulations, customer usage information is deemed to belong to the customer, and energy companies must obtain permission before they release it to requesting parties. State regulations should anticipate that situations may arise where data should be released in order to serve a reasonable request. For example, when people consider buying a home, it is plausible that they would want to know the current occupant's average monthly utility data in order to

[4]NIST IR 7628, released in September 2009 (NIST Cyber Security Draft 7268), p. 8. Available at http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf.

[5]NIST Cyber Security Draft 7628, p. 8.

[6]E.G. SEE ALSO, # 309; FTC Project No. P095416; FTC to Host Public Roundtables to Address Evolving Consumer Privacy Issues.

guide their decision. Whether or not energy companies may release such information, however, depends on state statutes and regulations. Thus, data release policies must be further refined to address situations where such release would be appropriate.

Up to this point, there has been little protection of energy usage data. For example, in Austin, Texas, law enforcement officials obtained access to individual energy consumption data in order to conduct computerized mass surveillance to identify anomalies in customer consumption and prompt investigations of possible drug production.[7] Despite the speculative and personal nature of the surveillance, the Austin Police Department remains "confident that the measures it utilizes follow the law."[8] A federal judge agreed, denying a motion to suppress evidence and stating that accessing energy data "does not violate any protected privacy interest."[9] Thus, there are existing gaps in the law that do not sufficiently protect the privacy of consumer energy information, either at the state or federal levels.

While states have been given authority to regulate electricity, the rising federal interest in the smart grid and the interconnected nature of the grid network could eventually result in a move toward national privacy regulations. Developing federal privacy protections for energy data may be advantageous because a national grid would likely be capable of sending data across state lines. Thus, the federal government may need to set a minimum standard of privacy protection, which states could build upon if they so chose, although states should still retain jurisdiction over energy privacy policy.

---

[7]Jordan Smith, *APD Pot-Hunters Are Data-Mining at AE*, THE AUSTIN CHRONICLE, Nov. 16, 2007, *Available at* http://www.austinchronicle.com/gyrobase/Issue/story?oid=oid:561535 (last visited June 24, 2010).

[8]*Id*.

[9]Order Den. Mot. to Suppress Evidence at 14, U.S. v. Colby, No. A-07-CR-072-LY (W.D.T. dismissed Nov. 6, 2008). See also, 62A Am, Jur. 2d Privacy § 5.

In its Smart Grid Policy Statement, the Federal Energy Regulatory Commission ("FERC" or "Commission") recognized the states' jurisdiction regarding smart grid while also acknowledging its federal authority in developing smart grid standards.[10] Addressing jurisdictional concerns raised by state regulatory entities, the Commission indicated "adoption of national standards for smart grid technologies should not interfere with a state's ability to adopt whatever advanced metering or demand response program it chooses."[11] The Commission added, however, that it has authority under the Energy Independence and Security Act of 2007 ("EISA") to "adopt smart grid standards—such as meter communication protocols or standards—that affect all facilities. . . if the Commission finds that such standards are necessary for smart grid functionality and interoperability in interstate transmission of electric power."[12]

The smart grid should not be put in place before these privacy principles are translated to specific norms, embraced by the industry, and properly enforced. Given that many states are already in the process of deploying advanced metering infrastructures capable of collecting granular energy usage data, privacy standards need to be developed immediately. While the state of smart grid privacy standards may seem rudimentary and jumbled at this time, there are already useful privacy frameworks available to develop enforceable and meaningful privacy rules, as discussed below. Even then, as with the general problem of cyber security, it may not be possible to stop all unauthorized access to customers' data. The public deserves to be educated about the risks that come along with the benefits of the emerging smart grid. This is not only good policy from the consumer perspective, it will be essential to attaining widespread public support for smart grid deployment.

[10]Smart Grid Policy Statement, 128 FERC ¶ 61,060 (2009) ("Smart Grid Policy Statement").

[11]Smart Grid Policy Statement at 17.

[12]Smart Grid Policy Statement at 15

COMMENTS

In general, for any program involving smart grid and associated technologies, NASUCA supports a voluntary opt-in program design and a national consumer privacy protection policy protecting personal energy information and the electronic transfer of such data. In response to the list of questions provided in DOE's Request for Information ("RFI"), NASUCA submits the following:

1. Who owns energy consumption data?

Utilities gain access to customers through highly regulated businesses, and infrastructure to provide their essential public services is paid through customers' payments of monthly statements. The information technology that is proposed to provide enhanced communications capabilities between customers and the utilities that is the foundation of the smart grid is likewise paid by ratepayers. Therefore, in the event that a utility installs smart meters, it should be clear that the customer must own her or his home energy usage data, have consistent access to that data for personal review in a usable format, be fully informed of what data is flowing to and from the meter, to whom the data is flowing, and with what frequency the data is communicated. Home energy data includes not only the energy used in the home but any energy generated from the home. Thus, customer generation data from a customer's distributed resource, such as solar panels, and net metering information should also be afforded customer privacy protection.

As mentioned above, home energy usage data may potentially reveal intimate details about an individual, including when the individual is home, what appliances he or she uses and how frequently those appliances are used, travel habits, socioeconomic status, typical food consumption, and when the individual is most likely to alter daily routines. Personal consumer information would appeal to many parties for a variety of uses, including energy companies

seeking to improve service, market additional services or sell aggregations of customer information for profit, third-party marketers, law enforcement agencies investigating possible criminal acts, insurance companies seeking to identify unhealthy behaviors in order to adjust rates, criminals reconnoitering to perpetrate illegal acts, researchers looking to create new energy-related studies, and competing businesses or manufacturers wishing to access business data of competitors. Companies have started to recognize the importance of privacy rights. For example, a representative from Google recently testified before Congress that "personal energy information belongs to consumers, and they should control who has access to it."[13] Thus, because an individual's home energy usage data is both personal and valuable, the consumer must have ownership of and access to and control of the consumer's own data.

2. Who should be entitled to privacy protections relating to energy information?

Consumers must be entitled to privacy protections regarding their personal energy information. As mentioned above, the customer is the ultimate owner of the customer's personal energy information, and as such the customer is entitled to privacy protections of this information. Customer information should be defined as all personally identifiable information (*e.g.*, account information used for billing purposes or unique device identifiers attached to an individual name) and data collected about an individual household (*e.g.*, granular usage data). Additionally, privacy protections should apply to all usage data capable of revealing personal-, household-, or organization-identifiable information.[14] The development of smart grid and

[13]Testimony of Edward Lu, Advanced Projects Program Manager, Senate Committee on Energy and Natural Resources Hearing on Smart Grid, March 3, 2009. Available at: http://www.google.com/powermeter/about/sgtestimony.html (last visited June 24, 2010).

[14]Organizations such as churches, schools, or political associations may warrant strong protections similar to those necessary to protect the privacy of individuals and households.

advanced metering technologies may dramatically increase the amount of information about personal energy consumption behavior that may be transmitted, communicated and stored, raising a host of privacy issues that may adversely impact consumers.

Privacy protections must explicitly protect consumers from unwanted use or disclosure of their home energy information, and they must be enforceable. Privacy rules should pertain to not only the utility or retail choice provider, or a demand response provider, but also to any third-party companies entrusted with the use of such information. Since the flow of data will often take place via electronic transmission, each time energy data is transmitted to a third-party, additional privacy and security risks arise. Thus, specific standards must be developed to protect the integrity of the transfer of customer energy usage information.

Customers should be permitted to choose their own degree of privacy protection, both with respect to information outflows and inflows. However, the ability of customers to choose the outflow of information should not impede the utility's ability to obtain the minimal level of information required to perform reliable operation of the grid, load research, or cost allocation assessment for rate design purposes. Any other customer-specific information about utility service and energy usage should not be made available to affiliates or third-parties, unless affirmatively authorized by the consumer or pursuant to a regulatory body order. There must also be appropriate safeguards for disposal or destruction of data after its usefulness has ended for the utilities, affiliates and vendees of customer data.

3. What, if any, privacy practices should be implemented in protecting energy information?

Smart grid design should prioritize a secure communications network with appropriate physical and other related safeguards to prevent security breaches and reliability deficiencies.

Privacy experts are now widely recognizing that the commonly used "notice and consent" model is inadequate.[15] Regulators must also recognize that ensuring privacy protections of energy information cannot be assured solely by gaining customer consent, nor by compliance with regulatory frameworks, but must be incorporated into organizational corporate culture. The DOE should consider the privacy principles and practices being developed by the Smart Grid Interoperability Panel Cyber Security Working Group, found in the National Institute of Standards and Technologies ("NIST") Draft Interagency Report 7628 entitled "Smart Grid Cyber Security Strategy and Requirements."[16] These principles and practices are:[17]

1) **Management & Accountability** - An organization should formally appoint personnel to ensure that information security and privacy policies and practices should exist and are followed. Documented requirements for regular training and ongoing awareness activities should exist and be followed. Audit functions should be present to monitor all data accesses and modifications, and the organization's incident response program should include specific procedures for energy usage data, as the smart grid is further deployed.[18]

2) **Notice & Purpose** - A clearly-specified notice should exist and be shared in advance of the collection, use, retention and sharing of energy usage data and

[15]For example, National Telecommunications and Information Administration Associate Director for Domestic Policy Daniel J. Weitzner recently stated "[t]here are essentially no defenders anymore of the pure notice-and-choice model." *See* Steve Lohr, *Redrawing the Route to Online Privacy*, N.Y. Times, Feb. 28, 2010, *at* Bus. 4, http://www.nytimes.com/2010/02/28/technology/internet/28unbox.html (quoting Mr. Weitzner).

[16]These principles are very similar to the Fair Information Practice principles recently adopted by the Department of Homeland Security. *See*, U.S. Dept. of Homeland Sec., *Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[17]Cybersecurity Coordination Task Group, *Smart Grid Cyber Security Strategy and Requirements*, Draft NIST Report 7628 (Feb. 2010), Available at http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628_2nd-public-draft.pdf, at 104-09.

[18]*Id*. at 104.

personal information. Any organization collecting energy usage data from or about premises should consider validating or adopting a process to notify the premises' inhabitants, and person(s) paying the bills (which may be different entities) when appropriate, of the data being collected, why it is necessary to collect the data, and describe the use, retention and sharing of the data. This notification should consider including information about when and how information may or may not be shared with law enforcement officials. Also, organizations should notify the recipients of services whenever any organization wants to start collecting additional data beyond that already being collected, along with providing a clear explanation for why the additional data are necessary.[19]

3) **Choice & Consent** – The organization should describe the choices available to individuals and obtain explicit consent if possible, or implied consent when this is not feasible, with respect to the collection, use and disclosure of their personal information. This notification should include a clearly worded description to the recipients of services notifying them of (1) any choices available to them about information being collected, and obtaining explicit consent when possible; and (2) explain why data items are being collected and used without obtaining consent from the individual (for example, needing certain pieces of information to restore service in a timely fashion).[20]

4) **Collection & Scope** - Only personal information that is required to satisfy the stated purpose should be collected from individuals. Treatment of the information

[19] *Id*. at 105.

[20] *Id*. at 105. While these draft principles reference implied consent, NASUCA has noted throughout these Comments its support for the adoption of affirmative consent requirements for disclosure of information.

should conform to these privacy principles. Collected data should be limited to that necessary for grid operations, including planning and management, improving energy use and efficiency, account management and billing.[21]

5) **Use & Retention** – Information should only be used or disclosed for the purpose for which it was collected, and should only be divulged to those parties authorized to receive it. Personal information should be aggregated or kept anonymous wherever possible to limit the potential for computer matching of records. Personal information should only be kept as long as is necessary to satisfy the purposes for which it was collected.

6) **Individual Access** – Organizations should provide a process for personal information data subjects to allow them to ask to see their corresponding personal information and to request the correction of perceived inaccuracies. Personal information data subjects should be informed about parties with whom personal information has been shared.[22]

7) **Disclosure & Limiting Use** – Personal information should be used only for the purposes for which it was collected. Personal information should not be disclosed to any other parties except for those identified in the notice, or with the explicit consent of the service recipient.[23]

8) **Security & Safeguards** - Personal information, in all forms, should be protected from loss, theft, unauthorized access, disclosure, copying, use or modification.[24]

[21] *Id*. at 106.

[22] *Id*. at 106-07.

[23] *Id*. at 107.

[24] *Id*. at 107.

9) **Accuracy & Quality** – Every effort should be made to ensure that the data usage information is accurate, complete and relevant for the purposes identified in the notice, and remains accurate throughout the life of the data usage information while within the control of the organization.[25]

10) **Openness, Monitoring & Challenging Compliance** – Privacy policies should be made available to service recipients. These service recipients should be given the ability and process to challenge an organization's compliance with their state privacy regulations and organizational privacy policies as well as their actual privacy practices.[26]

As an example of enhanced planning for privacy protection, Privacy by Design ("PbD") is a concept developed by Ontario's Privacy Commissioner, Dr. Ann Cavoukian, to address the protection of privacy across information and communication systems, business accountability practices and physical design of large-scale networked data systems. PbD is based on the following seven guiding principles, which DOE may want to take into account in forming smart grid policies:[27]

1) **Proactive not Reactive; Preventative not Remedial** – anticipating and preventing privacy invasive events before they happen.

2) **Privacy as the Default** – requiring no action on the part of the individual to protect the individual's privacy.

---

[25] *Id*. at 108.

[26] *Id*. at 108.

[27] Greater detail on the seven guiding principles is available at: http://www.privacybydesign.ca/background.htm.

3) **Privacy Embedded into Design** – embedding privacy into the design and architecture of IT systems and business practices by not adding privacy on after the fact.

4) **Full Functionality – Positive-Sum, not Zero-Sum** – seeking to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner.

5) **End-to-End Lifecycle Protection** – ensuring cradle-to-grave management of information from creation to termination of the information.

6) **Visibility and Transparency** – component parts and operations remain visible and transparent, to users and providers alike.

7) **Respect for User Privacy** – requiring architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Energy companies involved in the smart grid and state regulatory bodies may want to consider the use of Privacy Impact Assessment ("PIA") forms to guide their design process of a PbD. PIAs are mandatory evaluations that federal government entities must complete throughout the developmental process of a new system. While private corporations are not currently required to complete PIAs, the forms may provide a useful template that considers many different aspects of privacy protection. But given the substantial amount of federal funding allocated nationally to utilities for investment in smart grid technology development, an argument may be made that PIA's could be required of any entity underwriting with federal funding smart grid investment or seeking to utilize the smart grid for commercial exploitation. The following are some privacy-related questions that researchers and designers should consider to help guide the development of a PbD based upon the main points of PIA forms currently used

by federal agencies, such as the U.S. Department of Energy and the U.S. Department of Homeland Security:

1) **Collection of Data** – What are the intended uses of energy usage figures? What information is needed to achieve the goals of the grid? Can energy be collected in two forms: monthly billing info and energy distribution info?

2) **Storage and Encryption of Data** – Can personal information be encrypted or aggregated without affecting the overall goals of the system? Who will have access to this data and to what extent? How long will the data be stored in the system? How will stored data be accessed or searched? What protections are in place protecting against employee breach?

3) **Notice** – In a context where even websites struggle to provide adequate notice to users, how can designers give notice to something people have been doing for years through a product in someone's basement?

4) **Consent** – To what extent should consumers have to consent to giving data? Can users opt-out of the system entirely or, if that is not possible, limit their participation and the information they convey to the grid? Can the grid be effective if it utilizes only aggregated data?

4. Should consumers be able to opt-in/opt-out of smart meter deployment or have control over what information is shared with utilities or third parties?

Questions of whether or when to install smart meters, and under what conditions, should be addressed at the state level. In general, when a meter is replaced, whether as part of a wide-scale deployment of smart meters or due to a meter equipment failure, a customer could receive the smart meter currently being used by a utility. Smart meters may provide usage information

to the utility to enhance the proper operation of the grid. Smart meters have the potential of providing a more granular level of detail than is currently provided by existing metering technologies. However, to what extent this granularity of data is needed or wanted by the customer, the utility and third parties remains uncertain. Those benefits need to be quantified, not speculatively based on the total number of customers in the pool for meter conversion. Quantification includes establishing the cost effectiveness of the smart meters and the likely percentage of customers that may actively adjust their energy usage according to information concerning peak pricing.

Further, if or when smart meters are installed, it should be the choice of the customer as to what information can be shared, whom the information can be shared with and with what frequency the information can be shared. Although the consumer must own her or his home energy usage data, the data may be shared with the customer's authorized service providers upon the customer's decision to "opt-in" to a data-sharing arrangement. Additionally, the utility must maintain the ability to obtain the level of information required to perform reliable operation of the grid, load research, or cost allocation assessment for rate design purposes. With "opt-in" arrangements, the customer initiates the contact with the service provider and approves sharing the usage data with outside third parties. "Opt-in" means that customers cannot be automatically enrolled into data-sharing arrangements from which she or he must "opt-out" in order *not* to share the data with outside third parties. Through the establishment of an "opt-in" choice for consumers, ultimate ownership of the energy usage data remains with the customer, while third-party service providers must seek a customer's approval to use and share the individual customer data. And the ability to "opt-out" in the future must be preserved once an election to "opt-in" has been made.

Likewise, a customer should be allowed to choose whether she or he wants to be charged based on a dynamic pricing option basis, such as real time pricing or critical peak-time rebates, or retain a flat rate pricing which is not dependent upon a smart meter. The customer should have the choice to participate in dynamic pricing options if the customer believes there will be opportunities for greater savings compared to an alternative fixed rate.

5. What mechanisms should be made available to consumers to report concerns or problems with the smart meters?

Customer education is required to explain the deployment of smart meters, the enhanced communications abilities, the scope of information to be gathered, the possible additional uses to which that data may be employed, the ability of the customer to choose to participate in the gathering of the data and its sharing, the right of the customer to elect not to participate, the ability to revoke any prior election to participate, the telephone number of the customer service representative to whom calls about concerns or problems may be directed, as well as the telephone numbers of regulatory and advocacy entities in the jurisdiction to whom a customer may turn for additional assistance. All utilities and energy suppliers should be required to annually communicate electronically and in written hardcopy to customers the established mechanisms available to report any concerns or issues with smart meters and smart grid deployment. Initial communication can be in the form of a welcome kit once the customer "opts-in" or receives a smart meter. All customer bills should include a customer service hotline accessible both by phone and internet. Bill inserts may augment dissemination of the mechanisms in place to which the customer may resort.

While state commissions may have regulatory authority over utilities and licensed suppliers with regard to unauthorized disclosure or misuse of customer information, these

commission likely do not have the authority to address unauthorized disclosure or misuse by other third parties. As part of the education about smart meters, consumers should be provided information about the identity of the appropriate avenues for pursuing complaints in all of these situations.

6. How do policies and practices address the needs of different communities, especially low-income rate payers or consumers with low literacy or limited access to broadband technologies?

Policies need to be developed that recognize the unique differences among residential utility consumers that may be affected by the implementation of smart grid technology. The term "residential utility consumers" itself represents a vast array of different interests, socio-economic backgrounds, and demographics that necessitate careful and deliberate planning throughout the regulatory process. Policies should prevent the inequitable distribution of benefits that may occur when some customers benefit from the use of smart grid technologies at the expense of others. There is also a need to prevent the summary discounting of the use of smart grid technologies among low income and other communities, where the concepts have yet to be developed or shared. A properly planned smart grid program may result in the very real opportunity for all customers to obtain benefits over time.

Pilot programs will be needed to evaluate and assess the suitability of different smart grid technologies and associated pricing options among different residential communities representing a diverse economic makeup. Pilot programs are also needed to evaluate the practicality of offering different pricing options and incentives that result in conservation and consumer consumption behaviors among different customer communities. A systematic review of the different pilot program results will enable the adoption of best practices that can be applied as appropriate in different states.

There will be a significant need for public education associated with the deployment of smart grid technologies. This education effort needs to be a coordinated national effort involving all stakeholders, including local utilities, state commissions, consumer advocates, and grass-roots advocates that is coordinated with national policy principles and states. DOE could find it beneficial to sponsor workshops between the different stakeholders and state utility educators to develop strategies for educating consumers. However, the public education methods and messages must be adaptable to the state-specific circumstances and decisions regarding the deployment of smart grid technologies, and in particular, the use of smart meters.

The existing state mandated low-income assistance programs will likely need to be reviewed and potentially undergo modification to operate effectively in the new smart grid era. Several states offer billing options where low-income customers pay a percentage of income towards energy costs, or bills that are calculated using discounted rates rather than the actual bill. Utilities should be required to ensure that customers participating in low-income programs will be no worse off in the new smart grid world. There are possibilities for rebates, arrearage credits, or other incentives to be initiated based on the application of smart grid technologies. In addition, the access to real time usage information may prove beneficial in targeting the use of weatherization funding and the ultimate lowering of the financial assistance program costs. Any smart metering for low income customers should provide adequate incentives and means to achieve lower overall demand and cost.

7. Which, if any, international, federal, or state data-privacy standards are most relevant to Smart-Grid development, deployment, and implementation?

While states have been given authority to regulate electricity, the rising federal interest in the smart grid and the interconnected nature of the grid may eventually result in a move toward

national privacy regulations. Existing federal laws do not explicitly govern the collection, use or distribution of advanced metering data by government agencies. Such a national privacy policy may make sense because a national grid would likely be capable of sending data across state lines, and therefore it should set the minimum level of privacy protections. However, a state should not be prohibited from adopting more stringent privacy rules than any ultimately adopted by federal law. Thus, if a state had less comprehensive privacy regulations regarding the release of energy data to third parties, the default level of privacy protection established by federal law would govern. However, there should be no preemption of more stringent state requirements.

Any implementation of a smart grid project should meet federal and state requirements for cyber security[28] and protect the privacy of customer usage information, both with respect to usage data derived by the utility for customer billing and information obtained concerning a customer's specific usage of electricity. NASUCA agrees that both federal and state regulators have an important role to play in the development, adoption and implementation of smart grid practices that adequately protect consumers while maximizing the efficiency of the nation's energy grid.

8. Which of the potentially relevant data privacy standards are best suited to provide a framework that will provide opportunities to experiment, rewards for successful innovators, and flexible protections that can accommodate widely varying reasonable consumer expectations?

In addition to the discussion in response to question 3 above, customer data privacy standards must recognize the minimum data requirements utilities and energy service providers

[28]Cyber-security refers to the security of the information passing over the communications networks of the smart grid, and to the security of controls over system components, such as circuit breakers and other components of the system essential to the functioning of the grid. It also refers to the security of customer data (privacy), discussed below under Consumer Protection issues. Security may be compromised by equipment or operational faults, as well as intentional breaches by hackers, and unauthorized access to data and controls.

require for daily operations of the grid, and require that all smart meters provide, at a minimum, this level of detail to the service provider or utility.

9. Because access and privacy are complementary goals, consumers are likely to have widely varying preferences about how closely they want to control and monitor third-party access to their energy information: what mechanisms exist that would empower consumers to make a range of reasonable choices when balancing the potential benefits and detriments of both privacy and access?

Through exposure to real-time pricing information enabled by smart meters and an accommodating suite of available opt-in program designs, some consumers may have greater opportunity to save on energy expenditures in a manner directly suited to their individual lifestyle. With enhanced data communication technology, consumers should be given control over what data is shared through their privacy settings, and utilities should be able to accommodate varying degrees of participation by their customer base. Consumers should have a suite of privacy and "smart rate" designs to choose from, varying in the degree of information shared and real-time price/use exposure. Absent customer affirmation, the smart meter should only provide energy usage information that is communicated to the utility for grid management, reliability and billing purposes. In order to encourage the greatest participation, customers must be assured from the outset that privacy protections are in place, and about the level of security protecting their personal energy information from unlawful profiling or any non-authorized use.

Smart meters enable two-way communication and have the ability to connect with other "smart" devices, such as home appliances and computers. Smart meters are capable of communicating detailed metering and price information provided from the smart meter with an in-home management device through a HAN that would allow customers to share their personal energy usage information to their choice of demand-side management providers, including the

utility, demand response providers, *etc*. By encouraging the deployment of HANs and other in-home management devices, some consumers may gain greater control over their energy usage information than reliance on a single smart meter. The use of a HAN facilitates information communication between the smart meter, chip enabled communications in smart appliances and the consumer, and increases the ease of sharing data with energy services providers. To dispel notions customers are being controlled by "Big Brother," in-home energy management devices should be located within the home and in the sole control of the customer, and meet minimum security standards.

In addition to concerns specifically linked to protecting the privacy of consumer energy usage made available by smart meters, the smart grid and additional advancements in residential and commercial energy technology may permit more products and their usage information to connect to the grid, thereby expanding the types and amount of data collected. It is projected, for instance, that certain automobiles will eventually link up with the grid as their primary power source.[29] These Plug-in Hybrid Electric Vehicles ("PHEV") will serve as portable batteries that can store energy and send power back to the grid when it is needed. Storage methods like the PHEV will be crucial for the grid because of the increased use of more variable forms of energy production like wind and solar power. In the process of charging these new vehicles, the grid will also collect information regarding the traveling habits and daily schedules of consumers. This could only be the nascence of smart product expansion, and the grid's implementation may produce an entrepreneurial goldmine that already has inspired many new devices to connect with the grid, some of which will have the potential to relay even more personal information. Thus,

[29]David Weinburger, *The Grid, Our Cars and the Net: One Idea to Link Them All*, WIRED MAGAZINE May 8, 2009, *Available at* http://www.wired.com/autopia/2009/05/the-grid-our-cars-and-the-internet-one-idea-to-link-them-all/.

privacy protections need to be established in advance of the roll out of smart grid, taking into account future developments involving PHEV's and unforeseen devices, and the types, usage and amount of consumer information that may need to be determined and protected while using this new technology.

10. What security architecture provisions should be built into Smart Grid technologies to protect consumer privacy?

Any chosen architecture should have embedded cyber security, encryption, physical and operational safeguards. For example, encryption keys must be maintained in a secure location, employees must be trained in security and privacy rules and protocols, and employee access to security protocols should be controlled and limited. Further, smart grid technologies should support multi-point to multi-point communications. Regardless of the architecture structure used, NASUCA recommends development of open standard protocols that are vendor neutral.

11. How can DOE best implement its mission and duties in the Smart Grid while respecting the jurisdiction and expertise of other Federal entities, states and localities?

The Department of Energy could have an important role in identifying and sharing information about state utility and commission activities on smart grid and smart meter proposals. The state commissions should conduct a detailed analysis of the costs and benefits of their state utilities' proposed smart grid projects. Further, utilities should seek ARRA funds from DOE to reduce the cost impact on consumers of any approved smart grid deployment. Proposed smart grid projects should be addressed through state regulatory proceedings and should only be approved if the measurable benefits to utilities and ratepayers outweigh the costs. In the case where a smart grid investment is required to meet mandated policy goals, a least-cost/best-fit

analysis should be used. Such proceedings would weigh all the tangible quantifiable benefits leading to cost reductions from improved efficiencies accruing to the utility from smart grid deployment, defray any smart grid investment costs against the identified utility tangible cost-reduction benefits when considering any utility cost-recovery and develop estimations on consumer benefits from such investment that are susceptible to verification.

12. When, and through what mechanisms, should authorized agents of Federal, State, or local governments gain access to energy consumption data?

Federal, state, and local governments have no greater rights than third parties where consumer privacy protections are concerned and should be allowed access to usage data only upon consent of the consumer, or by court order. Law enforcement activity must proceed by the usual court procedures for authorizations to collect information from identifiable consumer data gathered by utilities for smart grid operations. When released for governmental or regulatory purposes, consumer data should be confidential. Exceptions may be allowed in the case of regulatory audits or in the processing of complaints by regulators.

13. What third parties, if any, should have access to energy information? How should interested third-parties be able to gain access to energy consumption data, and what standards, guidelines, or practices might best assist third parties in handling and protecting this data?

Third–party entities entitled to access an individual's energy information should be those which have agreed to state or federally adopted privacy rules, to whom the consumer has specifically authorized such access, to those who have been approved by state regulatory agencies or those who are working under the direct supervision of the utility. Other third parties that may request access to aggregated, non-specific consumer energy information could be, but

are not necessarily, limited to a retail choice aggregator of demand response, a regional transmission organization operating price responsive demand, or demand response programs supplier, governmental and academic researchers.

Third parties also potentially may receive access to individual consumers' energy information through a commercial relationship due to outsourcing of billing, customer service, technical support, data storage and retrieval management, *etc*., and all should be subject to privacy protections through contract agreement with the underlying utility or supplier. Any third party potentially entrusted with personal energy use information through indirect means should be clearly disclosed to the customer in advance of and with customer authorization before the actual disclosure. This disclosure would include the specific data that is being entrusted, the purpose for the use of the data, and what frequency the data is being communicated. Any information that is entrusted to third parties must be authorized by the consumer either directly or through required disclosures. Third parties should be subject to enforceable privacy rules (developed on the frameworks referenced in response to question 3 above). Additionally, there must be clear rules about permanently deleting all records of a customer's data when/if the customer ends service with the third party, or if the third party is dissolved for any reason. Many states already have statutory consumer protections that make it unlawful to divulge a consumer's telecommunications usage to a third party absent a court order. Similar statutory protections for the power industry should be developed by the states and adopted by DOE as part of its smart grid best practices.

14. What forms of energy information should consumers or third parties have access to?

Customers must have access to their energy usage data in a manner that is clear, understandable, useful and actionable. At a minimum, consumers should have access to their usage (both historical and current) and prices (both current retail rate and real-time price and for the previous day's equivalent time increment—if applicable for the pricing program selected by customer). Moreover, consumers should be able to access and review all data collected by the service provider. If the deployment of smart meters has been approved, data accessed by the customer may enable the customer to better manage customer's consumption of energy. There are a number of ways this information can be provided. For example, this can be achieved through the ability to compare use and usage patterns from different hours, days, weeks, months, and years. If the customer's current pricing program is linked to wholesale electricity prices, the customer should be able to view the real-time and day-ahead clearing prices representative of the customers' rate determinants. Ideally, the information accessed by the customer should have the option to be represented graphically rather than tabularly to assist the elderly and lesser educated populations of customers. Considering that weather is one of the primary drivers of energy usage and corresponding prices, consumers could also be provided with relevant weather information (both current conditions and forecasted conditions) so that consumers can plan for and adjust their use accordingly. However, the appropriate types and levels of information should be addressed by state commissions, based upon the type of smart meter deployment and with a consideration of the costs and benefits.

There are a variety of third-party service providers that may need or desire access to individual customers' personal energy information, such as demand response providers, outsourced customer service or billing specialists, as well as the local utility. For each of these

entities, however, the level of detailed information required varies significantly, as does the format of information received, and the frequency of access to the information. For example, the demand response provider may need real-time information to verify that the customer participating in a demand response program is in fact reducing load when called upon to do so. A customer service or billing specialist will need to be able to access the customer's account and past billing information and will most likely not have a need to access real time energy use. No reason can be contemplated for a retail customer on a fixed rate to be required to allow access to their individual real-time energy use. The customer should have the option to exclude access to this information if it is not relevant for the selected service or rate program the customer has chosen.

15. What types of personal energy information should consumers have access to in real-time, or near real-time?

Customers should have the proper information to manage their energy use in a way that results in the most savings to the customers. Customers should be enabled with the appropriate information to help them proactively manage their home energy usage. This includes not only knowing how much energy they are currently using and at what costs but how their current usage compares to yesterday's or other similar days and why. Customers should have the ability to recall their personal energy usage information, and information should be provided regarding conditions that day, such as average temperature, critical event days, peak or non-peak time period, historical hourly LMP prices, and related retail pricing information. This information can enable customers to assess what their "normal" energy use is throughout the day.

Current usage information may assist the consumer in evaluating daily activities in the household and the amount of energy usage associated with those activities. Cost of current use is

important to those that participate under a dynamic pricing rate structure, whereby the activities that consume the energy may be deferred until a lower cost interval of time to save energy costs for the household. Weather information, both current and forecasted, provides consumers notice of impending extremes in weather, which correlate with increased energy demand, and may yield benefits on demand response to offset the anticipated increased demand. Percent of peak load served at the current time by the local utility is information that corresponds to the extremes of weather experiences in summer and winter, and can signal appropriate time for voluntary deferment of energy usage as demand response. Graphical hourly representation of percent of peak load of the local utility, actual customer use, real-time and day-ahead prices that are correlated to any real-time rate the customer may be paying should be an alternative available to some customers not familiar with tabular displays, providing visual distinctions more easily understood.

Any smart meter deployment should be capable of utilizing a HAN that will enable the customer greater control over the types and amount of information that she or he wants to monitor. HANs are able to communicate with other appliances enabled with "smart chip" to display energy use and the cost of that use for each appliance. Residential customers have diverse needs and preferences. The integration of HAN could allow the customer greater flexibility to customize what personal energy usage information the customer wants to receive, the frequency of that information, and what format the information is conveyed in. Additionally, customers should have the ability to change any of their preferences without penalty or delay.

16. What steps have the states taken to implement Smart Grid privacy, data collection, and third party use of information policies?

Few states have legislated explicitly to implement smart grid privacy, data collection, and third party use of personal energy usage information policies. This is perhaps because the advent of smart meters and the federal impetus toward a smart grid has proceeded much more rapidly than state legislatures could anticipate the need for policies in these areas. Despite the lack of legislation pertaining explicitly to smart grid protections, however, many deregulated states have, through state statute and state administrative code similar to Pennsylvania, implemented policies requiring customer authorization prior to the utility releasing consumer information to a third party.

Additionally, states have taken further steps to protect consumer energy data. The District of Columbia, in its code, specifically limits the use of customer information (which includes any information about the customer and information provided to the utility by the customer) to the purpose for which the information was originally acquired, unless the customer consents to the use in writing.[30] In response to the privacy concerns related to smart metering, the Colorado Commission has opened an investigation, Docket No. 09I-593EG, in which it has sought comments from interested persons to a wide range of questions. The Commission is currently taking the comments under advisement.

Texas, in its utility code, has provided generally that customer consumption data is to be protected.[31] The Texas Public Utilities Commission has issued regulations to enforce the legislation. Under these regulations, a retail electric provider cannot release proprietary

[30]D.C. Code § 34-1507(b)(1).

[31]Texas Utility Code § 39.101(a)(2)

customer information to any other person (with exceptions including releases for consumer credit agencies, government law enforcement agencies) without the customer's verified authorization.[32] Further, the regulations prohibit a retail electric provider from selling, making available for sale, or authorizing the sale of customer specific data.[33]

Texas has regulated additional consumer protections when advanced metering is involved. For example, an electric utility must provide the customer, the customer's retail electric provider, and any other entity authorized by the customer read-only access to the customer's advanced meter data.[34] Further, an electric utility must use industry standards in providing secure access to the customer's data.[35]

17. What steps have investor owned utilities, municipalities, public power entities, and electric cooperatives taken to implement Smart Grid privacy, data collection, and third party use of information policies?

The answer to this question will best be obtained from utilities, municipalities, public power entities and electric cooperatives themselves.

18. Should DOE consider consumer data accessibility policies when evaluating future Smart Grid grant applications?

Smart grid technologies and program implementation are expensive and evolving. The extent of exploitation of the information that may be collected not only from smart meters but also from other smart appliances linked through HANs can only be speculated at this early stage

[32]Texas Public Utilities Commission Regulation § 25.472(b)(1).

[33]*Id*. at § 25.472(b)(2).

[34]Texas Public Utilities Commission Regulation § 25.130(j)(1).

[35]*Id*. at § 25.130(j)(3).

of smart grid evolution. To leave the significant issue of consumer data accessibility and its privacy implications until after significant smart grid investment would be unwise. Once consumer information is accessible beyond the utility's control, its further dissemination is inevitable. And, as victims of identity theft well know, once a consumer's private data has been released, it is practically impossible to get it back. Protections must be put in place at the forefront of development of the smart grid, and applications for grants for smart grid development must incorporate considerations of consumer data accessibility and privacy protections. Security and privacy assessments should be considered for any new smart grid technologies. Additionally, there is much work to be done in the area of educating utility customers about the smart grid and new rate design or pricing structures that will be enabled by smart meters. It would be premature to require any mandatory program participation exposing customers to real-time energy prices or unlimited access to customer information communicated through the smart grid. Further, there are other evaluation criteria that should have greater emphasis and be required for any smart grid program funding before there is wide scale deployment and utility customers are required to pay for them. Specifically, a detailed cost/benefit analysis identifying both operational and societal benefits of the smart grid deployment, a rate impact assessment on customer bills, and a benefits assessment to be derived by ratepayers should be performed prior to approval of a smart meter program at the state level. States must be permitted to retain authority over rate design and program participation associated with smart grid deployments.

CONCLUSION

WHEREFORE, NASUCA appreciates the opportunity to comment in this docket concerning smart grid and consumer privacy matters. NASUCA respectfully requests that the Department of Energy adopt the NASUCA's recommendations for the benefit of consumers.

Respectfully submitted,

NATIONAL ASSOCIATION OF STATE UTILITY CONSUMER ADVOCATES
8380 Colesville Road, Suite 101
Silver Spring, MD 20910
Phone (301) 589-6313
Fax (301) 589-6380