AARP Reply Comments to:

DEPARTMENT OF ENERGY
Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy

David Certner
Legislative Counsel and
Legislative Policy Director
AARP Government Relations and Advocacy

August 6, 2010

AARP submits the following comments on consumers and smart grid issues in reply to initial comments of a number of entities to the Request for Information (Request or RFI) on access to data in the smart grid space, published by the Department of Energy (DOE) on May 11, 2010.

About AARP

Founded in 1958, AARP is a nonprofit, nonpartisan membership organization that helps people age 50 and over improve the quality of their lives. AARP has offices in all 50 states, the District of Columbia, Puerto Rico and the U.S. Virgin Islands. For more than 50 years, AARP has been serving its members and creating positive social change through information, advocacy and service.

AARP's interest in this Request for Information derives from our advocacy on behalf of consumers in state utility regulatory proceedings and our understanding of the complexities of state utilities regulation and federal statutes. For more than 20 years, AARP has been the only national organization consistently working at the federal level and in the states to advance energy affordability and consumer protections from unfair utility policies and rate increases. Last year alone, our national and state office staff engaged in legislative and regulatory efforts in 30 states that resulted in millions of dollars in documented savings for consumers. AARP has also been involved in several state level proceedings on smart meter investments, including the recent Baltimore Gas and Electric proceeding in Maryland. In these venues AARP seeks to ensure that smart meter investment is cost-effective, does not put all investment risk on consumers and does not impose mandatory dynamic pricing on residential ratepayers.

Introduction

On May 11, 2010, the Department of Energy issued a request for information concerning *Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy*, 75 Fed.Reg. 26203. As stated in the summary of request, the purpose of requesting the information is:

> *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. This request for information (RFI) asks interested parties, including industry, consumer groups and State governments, to report on State efforts to enact Smart Grid privacy and data collection policies. This RFI also seeks input regarding individual utility practices and policies regarding data access and collection; third party access to detailed energy information; and the role of the consumer in balancing the benefits of access and privacy. Finally, this RFI seeks comment on what policies and practices should guide policymakers in determining who can access consumers' energy information and under what conditions.*

Dozens of interested parties filed responses to the RFI. AARP welcomes this opportunity to provide information to DOE concerning smart grid privacy and data collection policies, in response to the filings of several entities, including the National Association of Regulatory Utility Commissioners (NARUC), the National Association of State Utility Consumer Advocates (NASUCA), Edison Electric Institute (EEI) and the Demand Response Smart Grid Coalition (DSRG).[1] These entities capture a wide range of interested parties, from state regulators to consumer advocates, and from electric utilities to potential third party vendors over the smart grid.

AARP seeks to address two key issues raised in the comments of the entities noted above. In general, AARP believes that (a) consumer energy usage data (CEUD) as well as consumer identifying information must be provided a high level of protection from unauthorized access (particularly by remote parties not authorized explicitly by the consumer), and (b) the federal government should provide a floor, or minimum level of consumer protections, and not impose a ceiling on the protections states afford to electric consumer privacy. If the promises of the smart grid are to be fulfilled, consumers must be confident that they can participate in smart grid activities without risk to their privacy.

Are Privacy Protections Needed?

Most commenters agreed that consumer privacy is important and some level of protection is needed, as indicated by the following quotations from their initial comments:

> **DRSG coalition, answer to question 2:**
>
> Certainly energy consumers should be entitled to a high level of privacy protection. Utilities and other parties must utilize processes, procedures and technologies that ensure that a consumer's data is only accessible to the consumer, the utility and any third party that has been authorized by the consumer to have access.
>
> **Edison Electric Institute (pp. 2-3):**
>
> EEI's members stand for the rights and privacies of our customers, and recognize that preserving customer trust is essential to our success and to the success of third parties.

[1] Aclara, Advanced Telemetry, Ambient, Amplex, Bridge Energy Group, Boeing, CalAmp, CALMAC, Cisco, Comverge, Conservation Services Group, Cooper Power Systems, Corporate Systems Engineering, CPower, Direct Energy, Echelon, Eka Systems, eMeter, Energy Capital Partners, EnergyConnect, Energy Curtailment Specialists, EnergySolve, EnerNOC, Enfora, EnOcean Alliance, Enspiria Solutions, GE, Google, Honeywell, Ice Energy, Itron, Johnson Controls, KMC Controls, Landis+Gyr, LG Electronics, Lockheed Martin, Lutron Electronics, Oracle, PCN Technology, Sensus, Silver Spring Networks, SmartSynch, Space-Time Insight, Steffes, Tendril, Trilliant Networks, Tropos Networks, Universal Powerline Association, U-SNAP, Whirlpool, ZigBee Alliance, Ziphany.

NASUCA (answer to question 2):

Consumers must be entitled to privacy protections regarding their personal energy information.

NARUC (fifth whereas clause)

While the deployment of smart grid technologies may empower the consumer and provide more options, it also poses significant privacy issues that need to be considered and resolved by regulators.

All commenters essentially agree on the core principles that consumer privacy is important and some level of protection is needed. There appear, however, to be policy differences on the level of these protections and how they should be implemented. AARP agrees with NARUC that the deployment of smart grid technologies will pose significant privacy issues that need to be considered and resolved by regulators. But we go well beyond NARUC in our belief that both the federal government and state regulators must implement policies that assure that customer's personal and energy usage data will be protected.

AARP agrees with both DRSG and NASUCA in the belief that consumers are entitled to privacy protections, and further supports DSRG's assertion that consumers deserve a high level of protection sufficient to ensure that access personal data is restricted only to the consumer, the utility and third parities authorized by the consumer. AARP also agrees with EEI's assertion that privacy protections and consumer trust are essential to the utilities' success. We go beyond EEI's position, however, in our belief that assurance of privacy protection is essential to the success of the entire concept of smart metering. The overall benefits of smart metering and dynamic pricing have not been substantiated and remain open to doubt. As such, any lack of consumer confidence in the protection of their personal information will invariably undermine any technological benefits of advanced metering.

Federal vs. State Jurisdiction?

The question of federal state jurisdiction demonstrates considerable variance in the comments of the four entities. The range of comments on this question reflects the different institutional frameworks within which each commenter works, their views on the underlying issues of national standards vs. state authority, and their support for market activity vs. government oversight on behalf of consumers.

With respect to the federal role in promoting smart metering and setting the rules for privacy, the four commenters in question come out with an array of divergent views:

DSRG (answer to question 8):

> ... no single data privacy standard fits all needs. "Reasonable expectations" as to what information ought to be private vary from community to community. On the other hand, *having varying data requirements in different jurisdictions will thwart rather than promote innovation and experimentation.* The solution is to require a threshold of procedural safeguards, including meaningful disclosure and clear and simple opportunities to give or withhold consent, so that consumers empowered to make meaningful choices about the use of their data. *As long as these requisites are in place – information and choice -- privacy interests are protected* while leaving room for innovation and creativity (emphasis supplied).

EEI (at 31):

> ....privacy regulation of customer data has traditionally been the responsibility of the states, which have developed various privacy protection laws for customer data. Virtually all electric utilities have their own data ownership policies in accordance with regulations promulgated by state regulatory authorities. ...The NISTIR 7628 provides a thoughtful evaluation of the privacy exposures that may be created in Smart Grid environments, and helps to identify appropriate practices for meeting these new exposures. EEI recommends that the Department likewise view this NIST effort as a thoughtful approach to standards, guidelines, and practices for third parties in handling and protecting CEUD.

NASUCA (Introduction):

> 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.

NARUC (Fourth Resolved Clause):

> ...any Congressional or federal agency action should respect and incorporate State rules and ongoing State authority to protect ratepayers' privacy and ability to control access to their energy usage information...

The four positions above represent a spectrum of views on state/federal jurisdiction over privacy issues. NARUC asks that state rules and authority be respected and incorporated in any federal action on energy usage privacy. This amounts to a view that the federal government may issue privacy protection norms, but may not preempt any inconsistent state norms. AARP respectfully disagrees with the NARUC assertion. EEI is careful to note the historic state jurisdiction, but goes on to note that multi-state policies for smart grid privacy may be useful, and to point the

DOE in the direction of the NIST process for the specific policies it may consider. In other words, EEI does not take a hard and fast position on the federal/state issue, but leaves itself open to supporting the one or the other as the state and federal policies may be of use. AARP respectfully disagrees with this variance because we believe it is not in the customer's best interest.

Finally DRSG appears to take the position that the "reasonable expectations" standard should rule, and that the definition of this term properly varies from jurisdiction to jurisdiction, implying that states should set privacy norms. However, DRSG goes on to warn that inconsistent state standards will stifle innovation, meaning freedom for the demand response industry to develop offerings for and relationships with customers without regard to state privacy laws. DRSG proposes, in effect, that the federal government set a ceiling on the requirements a state may impose on the industry. [2] "*As long as these requisites are in place – information and choice -- privacy interests are protected* while leaving room for innovation and creativity (emphasis supplied)."

NASUCA asks that the federal government put a floor under privacy protection, so that state laws affording less protection would be preempted. AARP strongly supports the NASUCA position of a federal floor to protect privacy rights, but further encourages the federal government not act to lessen privacy rights afforded under state law. In other words, where federal law is stronger and provides more critical protections to consumer privacy, federal law should reign. If state laws are stronger and provide more critical protections, let state law prevail. Limiting privacy by federal fiat could potentially harm consumers and undermine confidence and support for the very thing the government is trying to promote: a modern grid infrastructure. However, a floor established by federal law to be further embellished by state laws should be the norm.

AARP believes that regulators and policymakers are right to take note that concerns about privacy protection may influence consumer behavior, and may also lead to inaction if consumers believe they have no control over what happens to their personal information. Thus, the importance of ensuring that privacy is meaningfully protected must be paramount as new technologies are developed.

Five kinds of privacy concerns are raised by implementation of a smart metering system.[3] These include identity theft, personal surveillance, energy use surveillance, physical danger, and misuse of data. In its recent draft interagency report on smart grid cyber-security, NIST has summarized these as "potential surveillance possibilities posing physical, financial and reputational risks." [4]

---

[2] This interpretation is confirmed by DRSG's comment at p. 6 that "in the residential sector model mechanisms, developed by NIST, FERC with input from DOE might be appropriate, with actual adoption, adaption and enforcement taking place at the state or utility level."

[3] Lillie Coney, *Privacy and the Smart Grid: How to Address Consumer Concerns Without Jeopardizing theGrowth of the Grid*, paper provided at interactive web conference of same name sponsored by Smart Grid Today, April 13, 2010.

[4] Second Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements – Feb 2010, at 101.

Privacy will be at risk not solely because of the particular data amassed through the smart metering system, but also by combining this data with other publicly-available data to produce specific personally identifiable information (PII) regarding a customer. Experts have demonstrated that with nothing more than raw interval metering data, a household's electricity uses can be identified with some precision. Using sophisticated tools, a person with access to smart meter data could determine intimate details of a household's life style, including for example the following:

- Are you home?
- Do you regularly go out at certain times of the day, week, month, or/and year?
- Do you have visitors?
- Have you set your house alarm system?
- Do you have a plasma TV?
- When do you bathe or shower?
- Are you asleep?
- What make and model of smart appliances do you use?
- Do you use an oxygen machine? Other medical equipment?

With smart metering, the consumer has no choice but to buy electricity, and no choice but to buy it through the utility, whose smart metering and data collection pose the risk of a breach of their privacy. The customer will not be able to opt out of the collection of such data, nor of its communication over the utility's communication networks.[5]

A nuanced and careful policy is, thus, required to assure consumer rights. AARP believes that some states may be in a better position than the federal government at present to assure such privacy rights and tailor them to community concerns. Many States and provinces have taken up the question of privacy and smart metering. They should be given an opportunity to work through the complex questions of data access that arise in the case of smart metering. Federal action at this time could be helpful in setting a floor for customer protection and encouraging State action. But it can also serve to stifle State efforts and discourage policy innovation. However, the federal government's role should not promote smart metering innovation and related markets by limiting or undermining consumers' expectations of personal privacy. Weak national standards as a ceiling on consumer rights will only deepen the growing sense that many consumers have that smart metering is not in their interest.

Consumer outcry over the impact of new meters and pricing plans in California and Texas underscores our concern that the roll-out of new technology has sped ahead of the necessary development of consumer protection policies. Indeed, as evidenced by recent industry meetings,

[5] It is not clear whether the consumer can prevent her data from being communicated over the internet to the utility's web portal, whether or not she accesses the data.

utilities and smart meter vendors have begun to realize that they have left the consumer out of the equation in smart meter deployment and are playing catch up. [6] State regulators are now beginning to consider consumer protection and privacy concerns as part of their review and approval of smart meter deployment.

Conclusion

Historically, utilities have not been involved with issues such as profiling, tracking and third-party data transfers, because their existing business models have not included databases of significant, non-billing customer information. However, with implementation of smart meters, a host of issues arise relating to managing privacy issues for new types of data. Customers must feel safe in their data transfers and know that the data once made available under the customer's authority will neither become lost to the customer's control, nor circulated at the vendor's discretion for its own profit.

Therefore, it is crucial that privacy is addressed in a manner that ensures a minimum federal guarantee that personal customer information and usage data will be protected from unauthorized access, and that federal efforts to promote smart metering innovation and implementation not limit the ability of States to enhance protections for electric customer privacy. The extremely high value of such data to marketers, debt collectors, scammers, and crammers makes such information particularly susceptible to misuse. Unless access to data is avidly protected, consumers' personal and financial privacy and even their safety could be at risk. Strict safeguards should be adopted, adhered to, and regularly reviewed for appropriateness and effectiveness to guarantee that the consumer is entitled to the highest level of privacy. Those safeguards will do much to advance the success of smart grid technologies.

[6] http://www.demandresponsetownmeeting.com/home/, last viewed June 23, 2010.