U.S. Department of Energy Smart Grid Privacy Workshop Summary Report

January 31, 2012

Hosted by:
Dow Lohnes PLLC

Prepared by
Energetics Incorporated

ENERGETICS
A Subsidiary of VSE Corporation

TABLE OF CONTENTS

INTRODUCTION

As smart grid deployments have increased throughout the United States, concerns regarding consumer access and privacy related to consumer energy consumption data have become increasingly important. In response to these concerns, a multitude of entities have launched activities, including state commission proceedings implementing privacy principles and the development of potential models by federal agencies and private enterprises. Through these efforts, significant agreement appears to have been reached on fundamental issues, such as the need to protect individually identifiable information and the need for informed consumer consent. While all of these efforts are valuable, a patchwork of varying legal requirements can create uncertainty and unnecessary complexity for both industry personnel and consumers. Therefore, the U.S. Department of Energy (DOE) saw a need to convene stakeholders from the electricity industry to identify concerns relating to consumer access and data privacy and to discuss possible mechanisms to address these concerns.

To provide a collaborative environment for a variety of stakeholders to express their thoughts, opinions, and perspectives on smart grid consumer data privacy, DOE hosted the *Smart Grid Privacy Workshop* on January 31, 2012 at Dow Lohnes PLLC in Washington, DC. More than 80 representatives from several stakeholder groups attended the meeting. Participants represented 16 utilities, 15 third-party vendors and carriers, 12 consumer advocate organizations, 3 state commissions, and 9 federal agencies. DOE convened the meeting in order to gain a comprehensive understanding of the issues and to hear stakeholder perspectives and recommendations for a path forward. The specific purposes of the workshop were the following:

- To facilitate a dialog among key industry stakeholders regarding consumer electricity data access and privacy
- To identify key issues, ongoing activities, and specific areas of concern
- To determine if a national privacy strategy could help coordinate efforts and provide leadership
- To identify specific actions or approaches, including privacy protection regimes used in other industries, which could be part of a national strategy to resolve key priority issues

The workshop began with an overview of several ongoing activities to provide a snapshot of the current landscape and to lay the foundation for discussions. After hearing about the current activities, participants were then divided into breakout groups for facilitated discussions. Each breakout group was carefully constructed to have an equal mix of stakeholder representatives (utility, vendor, consumer advocate). Individuals from various federal agencies observed the discussions and provided background information. The workshop centered on facilitated discussions on the following four topics:

- The value of smart grid data
- Key smart grid privacy issues
- Potential activities needed to address the key issues
- Advantages, disadvantages, and next steps of a national privacy strategy

These sessions were led by professional facilitators, who guided participants in structured brainstorming and critical analysis to identify the most significant issues and build agreement on options and approaches to moving forward. The groups then reconvened and each breakout group provided a report on their groups' discussions and results.

KEY FINDINGS

Overall, participants were pleased with the meeting and its format. Participants appreciated the opportunity to hear other stakeholder perspectives and to discuss the issues in a constructive and collaborative manner. Through the discussions, several key recommendations emerged.

- The Federal Government should facilitate the development of a consumer data privacy framework. The framework should
  - Provide guidelines not mandates
  - Be developed through a Collaborative process involving all stakeholder groups
  - Define jurisdictional lines (state versus federal)
  - Define consumer consent
- Develop and compile an information library of ongoing activities that can be used and accessed by all stakeholders
- Determine and promote best practices
- Provide education to consumers to help them understand the value of the data, what consent means and the reason for grid modernization efforts
- Compile and disseminate lessons learned
- The Federal Government should act as a convener to bring together stakeholders to discuss key issues surrounding privacy and share information and solutions

MEETING RESULTS

Summary of Ongoing Activities

Many activities are currently taking place to address consumer data privacy. Some of those activities were highlighted at the meeting.

Establishing a Framework for Third Party Access to Consumer-Specific Energy Use Data
Michael Pryor, Dow Lohnes PLLC

The 2010 DOE report *Data Access and Privacy Issues Related to Smart Grid Technologies* identified the issue of third-party access to consumer-specific energy use data (CEUD) as one of the most critical questions in the context of Smart Grid technologies. In preparing the report, DOE collected comments from a broad range of stakeholders interested in the development of innovative Smart Grid technologies based on the availability of highly granular energy consumption data. These stakeholders reached consensus on several privacy and access questions, including the need for consumer education and empowerment and the consumer's right to control third-party access to CEUD (for example, by requiring utilities to obtain consumer consent before sharing CEUD with third parties).

Several states, including California, Texas, and Colorado, are now moving to implement Smart Grid privacy and data access policies. In July 2011, the California Public Utilities Commission (CPUC) adopted rules to protect the security and privacy of data generated by smart meters, including policies to govern access to customer usage data by consumers and authorized third parties. The rules apply to three major electric utilities, third parties under direct contact with the utility to conduct a primary purpose, third parties that the CPUC authorizes or funds to perform a primary purpose, and customer-authorized third parties who acquire data directly from the utility via an Internet connection pursuant to tariff.

NIST Smart Grid Interoperability Panel Activities
Marianne Swanson, Senior Advisor for Information System Security, National Institute of Standards and Technology

The Smart Grid Interoperability Panel (SGIP) is a public/private partnership that comprises more than 700 member organizations representing 22 stakeholder categories, including federal agencies and state and local regulators. Its Cyber Security Working Group (CSWG) works to develop a cyber security risk management strategy for the Smart Grid to ensure the interoperability of solutions across different domains and components. Several CSWG sub-teams are working to address Smart Grid privacy issues. The CEUD Privacy Protection Team has drafted recommended practices for third party access to CEUD. The Privacy Use Cases Team has incorporated privacy considerations and checks into use cases included in *Guidelines for Smart Grid Cyber Security* (NIST Interagency Report 7628). The Smart Grid Privacy and Training Awareness Team is creating multiple sets of "train the trainer" slides to help those who train smart grid entities (utilities, public utility commissions, and so on) to understand and address privacy implications of the smart grid.

Green Button Initiative
David Wollman, Deputy Director, Smart Grid and Cyber-Physical Systems Program Office and Manager, Smart Grid Standards and Research, National Institute of Standards and Technology Engineering Laboratory

In September 2011, U.S. Chief Technology Officer Aneesh Chopra challenged utilities across the country to quickly develop a "Green Button" that would provide consumers with simple online access to their detailed energy usage information. When a consumer clicks on the Green Button, the consumer's computer

downloads energy usage information in a standardized human- and machine-to-machine readable electronic xml format. This streamlined access will make it easier for consumers to engage with third parties offering services and products to help them understand and take action to better manage their energy usage.

With support from the Office of Science and Technology Policy (OSTP), the National Institute of Standards and Technology (NIST), and DOE, the three largest utilities in California have voluntarily responded to this challenge and have worked together with NIST/DOE/OSTP, with the approval of the CPUC, to coalesce around an initial common electronic format, based on nationally recognized voluntary standardization efforts. The California utilities have made significant progress and are now implementing the Green Button for their customers, with two of the three utilities offering the capability as of mid-January 2012.

Department of Commerce Activities
Ari Schwartz, Senior Internet Policy Advisor for the NIST Information Technology Laboratory, U.S. Department of Commerce

The Department of Commerce strives to ensure data privacy, security, and copyright while also encouraging the free flow of information. The Department's Internet Policy Task Force issued a report, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, detailing initial policy recommendations aimed at promoting consumer privacy online while ensuring the Internet remains a platform that spurs innovation, job creation, and economic growth. The report outlines a dynamic framework to increase protection of consumers' commercial data and support innovation and evolving technology

Based on extensive public input and discussion, the report recognizes the growing economic and social importance of preserving consumer trust in the Internet. The report also notes that the nation's privacy framework must evolve to keep pace with changes in technology, online services and Internet usage. The following are key recommendations:

- Consider Establishing Fair Information Practice Principles comparable to a "Privacy Bill of Rights" for Online Consumers
- Consider Developing Enforceable Privacy Codes of Conduct in Specific Sectors with Stakeholders; Create a Privacy Policy Office in the Department of Commerce
- Encourage Global Interoperability to Spur Innovation and Trade
- Consider How to Harmonize Disparate Security Breach Notification Rules
- Review the Electronic Communications Privacy Act for the Cloud Computing Environment

Future of Privacy Forum
Jules Polonetsky, Director and Co-Chair, Future of Privacy Forum

The Future of Privacy Forum is an industry supported think tank with an advisory board of corporate Chief Privacy Officers, academics, regulators and privacy advocates. Together with a number of leading companies it is creating a third party enforcement and seal program to provide additional oversight and assurance for secondary uses of energy data that is collected directly from consumers or provided by utilities or smart meters to third parties with consumer permission. A third party privacy seal program can play an essential role by vetting the privacy standards of third parties and by providing assurance to utilities, regulators and consumers that companies are in compliance with responsible standards. A third party seal can also provide consumers with an avenue for complaint handling and resolution and provide regulators with a supplement to their efforts to ensure consumers are protected.

State Energy Efficiency Action Network
Michael Li, Special Advisor for Electricity Policy, Office of the Secretary, U.S. Department of Energy

The State and Local Energy Efficiency Action Network (SEE Action) is a state- and local-led effort facilitated by the U.S. Department of Energy (DOE) and the U.S. Environmental Protection Agency (EPA) to take energy efficiency to scale that builds on the foundation of the National Action Plan for Energy Efficiency. SEE Action offers knowledge resources and technical assistance to state and local decision makers as they seek to advance energy efficiency policies and programs in their jurisdictions, with the goal of SEE Action achieving cost-effective energy efficiency by 2020.

SEE Action's Customer Information and Behavior Working Group promotes the use of energy information and feedback to change residential energy consumption behavior and achieve deeper energy savings in two ways. First, by providing tools and resources for regulators and policymakers about data access and privacy issues associated with energy efficiency. And second, by supporting the development of uniform methods to measure energy savings from energy efficiency programs targeting behavior change. The Working Group develops an array of resources to educate, engage, and support energy efficiency policy and program adoption, including a guide to data access and privacy that highlights issues related to how customer energy usage data is provided to third parties for efficiency purposes.

NARUC Activities
Robin Lunt, Assistant General Counsel, National Association of Regulatory Utility Commissioners

Privacy issues are important, but addressing them can be complicated. Getting these issues right will determine how consumers respond to the Smart Grid. States are beginning to address the issues.

NARUC established a Smart Grid working group to analyze smart-grid issues that will interact with the federal government and other stakeholders. The Smart Grid Working Group consists of seven State utility regulators who represent the Association's geographic diversity and most relevant committees—Electricity, Telecommunications, Energy Resources and the Environment, Critical Infrastructure, Consumer Affairs, and the Executive committees. NARUC formed the Working Group to serve as the central focus for communication both within the Association and to outside groups such as federal agencies, consumer groups, and other industry stakeholders.

NARUC has also established a dialogue with the Federal Energy Regulatory Commission (FERC) Electricity Committee regarding Smart Grid. The mission of the FERC-NARUC Collaborative on Smart Response is to provide a forum for Federal and State Regulators to discuss Smart Grid and Demand Response policies, share best practices and technologies, and address issues that benefit from State and Federal collaboration.

Privacy by Design
***Dr.** Ann Cavoukian, Information and Privacy Commissioner, Ontario, Canada*

Privacy by Design (PbD) is a concept developed by Dr. Ann Cavoukian in the 1990's which advocates embedding privacy into an organization's operations and into the design specifications of various technologies. The approach encompasses three areas of application: (1) information technology; (2) business practices; and (3) physical design and infrastructures. Privacy by Design is predicated on the idea that embedding privacy principles into an organization's operations and design is a better method than trying to address privacy assurance solely through regulatory frameworks. By making privacy the default setting within an organization, its customer's are automatically protected.

The 7 Foundational Principles of Privacy by Design are:

1. Proactive not reactive; preventative not remedial - Recognition that privacy interests and concerns must be addressed proactively;

2. Privacy as the default - Application of core principles expressing universal spheres of privacy protection;
3. Privacy embedded into design - Addressing privacy concerns when developing information technologies and systems, throughout the entire information life cycle —end to end;
4. Full functionality- positive sum not zero sum - Not trading off privacy for security in system design and instead ensuring both privacy protection and system functionality
5. End-to-end life cycle protection – Recognition that protection of collected information must persist throughout the entire process from start to finish
6. Visibilty and transparency – Operating according to the stated promise and objectives, subject to independent verification; and
7. Respect for users' privacy – Keeping the interests of the individuals uppermost by offering such measures as strong privacy defaults, appropriate notice and empowering user friendly options.

Through a long succession of advocacy, guidance, and collaborative initiatives, the IPC's office is ever increasingly involved in assisting public and private sector organizations understand the importance and need for the Privacy by Design approach. This work has led Privacy by Design to be adopted as a standard by the International Association of Privacy Commissioners and Data Protection Authorities, an entity that represents privacy authorities around the world.

The Value and Need for Energy Consumption Data

The breakout groups began their sessions discussing the reasons for and against providing access to consumer electricity consumption data. Overall, the groups agreed that there is value both to the consumer and to utilities for having access to electricity consumption information. For the end user, this data will provide more information to help them better manage their usage. For utilities, this data will improve operations and efficiencies, which will ultimately benefit the consumer in many ways, including possible cost savings and improved reliability and outage management. Participants noted that these benefits need to be communicated to the public so they can better understand the individual and societal value in having this information made available to them.

Issues that were raised against providing consumer electricity consumption data centered on concerns that the data will not be handled properly and securely once released, and to whom the customer would have redress if the data was mishandled or breached... No concerns were raised that sharing this data in any way lacked value. However, other reasons for not providing this data included needing to determine and reveal upfront how the data is going to be handled and how it is going to be securely transmitted. Also, utilities and vendors might be reluctant to provide access to this data based on questions of liability. Participants stated that these issues need to be addressed and resolved for consumers to feel comfortable sharing their data.

The Identification of Key Smart Grid Privacy Issues

For the second focus question, the groups defined the most significant privacy issues that must be resolved to ensure consumer trust and acceptance of smart grid technologies. All the groups recognized the importance of educating consumers to help customers become comfortable and confident enough to have their data released. Education will also be required regarding how the data will be used to help improve grid operations and how end users can use the information to better manage their electricity use. The groups also agreed that it was important to gain consumer consent prior to the data being released to a third party. Consumers need to be aware how third parties will use the data in order to feel confident in the security of data transfers and to understand who controls the data at each transfer point. Another common issue was the question of who has jurisdictional oversight of the data (state versus federal). One breakout group also raised the issue of cost considerations. Table 1 summarizes the top privacy issues identified by each breakout group.

Table 1. Summary of Top Key Smart Grid Privacy Issues as Identified by Each Breakout Group				
Group 1	**Group 2**	**Group 3**	**Group 4**	**Group 5**
• Need to **educate consumers**—not just about privacy but the value of the data • Need to create **privacy protections** without stifling the market and innovation • How to **police the bad actors** that don't protect the data?	• What does **informed consent** look like from the consumer's perspective? Who owns the data? Who maintains it and for how long? • What are the **touch points as the data moves**? At each hand off (e.g., utility to consumer, consumer to third party) who owns it? Who has **jurisdictional oversight**? • Value to consumer is driven by how they see the value of smart grid	• Cost considerations: Recognition of best practices; high-level principles • Federal strategy yes, but not too prescriptive • Customer education: Consumers need to feel comfortable that their information is kept private. They need to understand their choices. • Third-party usage	• Consumer education • What are the value propositions? Need to explain the importance of modernizing the grid. • Need to communicate the benefits (OMS, etc.). • When educating, do not lead with privacy issue • How can a utility use/share customer data without consent and which uses should require consent? • Who is responsible for oversight of third parties? ••• • Who engaged? • State/federal? • Generic privacy protections might work to develop oversight of third parties, etc.	• Communicating with and **educating customers** • Need for **informed consumer consent** prior to release of data to third parties • Security of data transfers • Data granularity – can the data be used to identify specific consumers? • **Federal versus state jurisdictional** oversight/areas of rights/ responsibilities

Mechanisms and Activities for Addressing Issues/Activities

The groups then discussed the mechanisms and activities that could be used to address key issues. A common mechanism identified by each group was consumer education which can be used to explain the value of sharing electricity consumption data, to strengthen consumer understanding, and to provide information on what "consent" means. Another suggested activity is to define baseline privacy protection requirements. This would include describing what informed consent means and what it looks like. It would also include defining who has control of the data, using protocols from the federal level as a framework. In this way, the government provides direction but does not mandate what to do, so privacy guidelines remain flexible, provider-friendly, and can be adapted for each state.

Finally, the groups suggested taking a survey of the existing landscape of activities (for example, in California), of the policies that are currently in place, and what was done in other industries (such as banking

and cellular communications), which could be used for defining pros and cons, and for sharing best practices and lessons learned.

The breakout groups identified dozens of prospective activities, which can be grouped into 9 distinct categories: Consumer Education, Federal Government as a Convener/Facilitator, Develop a Framework, Informed Consent, Lessons Learned, Map the Data Path, Survey what's Already Being Done, Determine Jurisdictional Lines, and Other. Below is a consolidated list of possible activities that resulted in the brainstorming discussion. The bullet text is taken directly from the raw output of each facilitated sessions, presented in full in Appendix 3. To illustrate interrelationships, a sub bullet structure has been imposed to draw connections between activities.

Consumer Education

- We need an education campaign on smart energy use; why you should care (aka smart grid capabilities)
  - Customer education focused on benefits, show them the purpose
  - Define for the customer what data will be collected, how it will be used, and how it will be protected
  - Define value propositions for difficult customers
    - Messages should be easily understandable and come from a trusted party
    - Define the pros and cons of opting-in or opting-out
    - Benefits should be the leading message
    - Explain the importance of modernizing the grid
- Create an education collaborative
  - Extensive, multi-faceted customer education programs and engagement are needed across all stakeholder groups, including utilities, government agencies, private entities and vendors.
  - Government as a convener of an educational campaign. Engagement through social media and apps contests
    - Hopefully, demands for smart grid improvements will come from consumers wanting it. However, consumers need someone to explain the value to them
  - Understand motivations and interests of stakeholders (basis for consensus building)
  - Customer education activities
    - Web and media campaigns that highlight the benefits to customers and utilities
    - Third party usage
    - NAESB Requirement 22 is a model
    - Business practices guide
  - Explain value to consumers (e.g., cell phones have significant radio frequency radiation and privacy concerns, but customers see the value of the product. Smart grid privacy issues will go away when customers see the real value of smart meters. Otherwise, there will be pushback).
  - Convene focus groups—ask consumers what they are looking for, what would make them use this, or not
  - Develop consumer education case studies; what has worked, what has not

Federal Government as a Convener/Facilitator

- Consensus building—get buy-in
- Involve multi-stakeholders
- DOE should provide forums for utilities and state rule makers
  - Share information on solutions to customer problems
  - Share ideas/experiences/solutions
  - Share customer education efforts
- Industry events to openly share best practices and lessons learned in consumer engagement and technology deployment

Develop a framework

- Clear rules of the road would make it easier to raise consumer awareness. We need more than just voluntary practices
- Flexible, provider-friendly privacy guidelines or protocols—not regulations or statutes
  - Vendors are concerned that there might be a lot of jurisdictional-specific rules and regulations that would make it hard to do business nationwide. What is needed is a nationwide privacy undertaking that has real enforcement without a comprehensive regulatory regime. (Regulations from the U.S. Department of Energy or the Federal Trade Commission are very prescriptive and too rigid. Regulations should accommodate different privacy tolerances.) Companies can commit to this undertaking, and receive a seal/icon that provides comfort to consumers
- Establish and maintain national standards for data sharing and communications
  - Develop a national privacy policy that presents minimum protections, preserves PUC authority to implement, and establishes privacy certification for third parties that is not jurisdictional
    - Federal government could define baseline privacy protection requirements
    - A consistent nationwide minimum that's communicated nationally
    - Build on established fair information and privacy standards
    - Use generic privacy protections
    - Define the basic information that utilities need to provide safe, reliable service
    - Customer cannot opt out of providing this information to the utility
    - Define what is personally identifiable information (PII).
    - Evaluate risk
    - Determine guiding principles and core benefits
      - Cascade to detail and prioritize
      - What is the vision?
      - Principles can be shared across utilities, etc.
    - Privacy policy should cover data, not just smart grid data
    - Clear rules on data; the rules must be clear, and the customers have to buy in. It doesn't matter if it's state or federal

- Continue to update privacy policies to accommodate new technologies and changes in law
- Develop privacy policy that defines who is responsible for data security and privacy after data leaves a utility's control
  - State PUCs regulate utilities and provide consumer's with the means to file a complaint and provide remedies, so who is responsible for enforcing data security and privacy protections after data leaves the utility's control?
  - If the consumer has the data and controls the data release, what are the rules?
  - The personally identified data belongs to the customer
- Develop rules and regulations to address control of the data by third parties
- Develop a national policy for defining customer-specific data; recommendations for informed consent procedures
- Develop a certification process to verify customer authorization
  - Establish a point of contact for questions and complaints
  - Can allow consumers to trust that wrong parties won't have access to the data
- Data security—federal input/guidance/requirements are needed. There is a need for processes to integrate federal and state utility regulation in cyber security and interoperability. Feds are not doing effective outreach to state entities that don't have the time or resources to participate.
  - There is a timing disconnect between the multiple groups on the federal level and the states where meters are being deployed. (For example, in MD, there are work groups looking at cyber security and privacy issues.) There is a need for a simpler process to integrate parallel federal and state processes in order to assist state efforts. States might not have the expertise, so the federal government can help
- Develop a seal program to implement voluntary enforceable codes on FIPs (fair information practices) via multi-stakeholder process
  - Crosses jurisdictional boundaries

- Define a framework that allows states the flexibility to implement oversight
  - Mandate that the state commissions have cost recovery mechanisms to help utilities implement standards and build infrastructure to support the delivery of information to customers and third parties
- Certification and regulation of third parties
  - Develop best practices for third party data
    - A standard for how those third parties deal with data if it is considered sensitive enough that it needs to be protected
  - Develop guidelines and rules for third party companies to transfer, receive, and secure data
  - Identify consumer complaint options, remedies and points of contact
- Address rate structure and universal service issues
  - Smart electric rates (time of use, dynamic pricing) critical to a market with electric vehicles (enabling)
  - Principle before prescription
  - Define roles and responsibilities of stakeholders

- Develop a methodology for embedding privacy by design into processes to minimize rules and regulations for what you are trying to accomplish

Informed Consent

- Informed consent—data release. This is a state issue in terms of regulations and utility protocols, which are needed. This could be encouraged at a national level, but it should come from the bottom instead of the top
- Develop a mechanism for consumer to file a complaint with misuse or breach of data
- Stakeholder can identify opt-out data fields and uses

Lessons Learned

- Document best practices (utilities, industries, and states)
- Don't recreate the wheel, use or build on privacy standards and language that is already in place for telecommunications and the internet
    - Research privacy policies that are already in place in other industries
        - Understand why different sectors handle privacy differently
        - States have different perspectives on privacy
    - Perform studies of approaches (privacy building blocks) and understand trade-offs
    - DOE should talk to the Federal Communications Commission regarding customer choice and best practices
    - Incorporate from other industries what they have done in terms of privacy and consumer engagement (e.g., banking, iPhone); we can learn from their mistakes, e.g., no one understands banking privacy notices
        - The electric distribution industry is heavily regulated. It's a different model than even telecommunications, because consumers only have one option.
        - People used to be afraid of putting their credit card information on the internet.
        - There is a federal law that limits consumers' exposure to credit card fraud. But is there a comparable backstop for electricity consumption data? This could lead to problems. For example, a landlord could look at usage profiles when choosing tenants.
        - This is not necessarily a new challenge. Browser and internet use data are comparisons. Companies and courts have figured out how that data can and should be released.

Map the Data Path

- Identify how data flows from the meter to the utility or customer and then to a third party for purposes of identifying applicable jurisdictions, regulation and areas where we have gaps in consumer protection
- Perform scenario analyses
    - Walk through what concerns consumers
    - Are consumers getting what they want?
    - Look at what goes on at trade shows and state commissions
- Define security standards for data transit

Survey What's Already Being Done

- Thoughtful study of issues (facts on tech, existing policies, policy goals)
- DOE should develop a comprehensive survey of existing privacy policies and practices in the states and utilities
- Utilities need to review their existing privacy policies and procedures, and update them as needed in relation to NAESB best practices and standards

Determine Jurisdictional Lines

- Decide whether this will be managed at the state level or federal level
- Determine the proper roles of the federal government and state governments (e.g., in regard to technical protocols, business rules)
    - For example, states defer to the federal government on technical protocols for cyber security and interoperability, but states take the lead on business rules and practices for retail electricity sales
    - This is a role issue. Federal agencies have roles (oversight, regulation), and so do states
    - Indeed, the federal government doesn't understand the full plan or fully appreciate what already exists on the state level

Other

- Industry Button—give the data over to customers in a standardized format that the customer can send it to a third party vendor, the utility is out of the equation
    - Relatively simple process
    - Reduces utility from liability of handling that data
- Innovation more than educating people; you have to create a market, user interface matters
- Encourage utilities to activate the capability of smart meters to communicate with HEMs
- Study the possible use of a "permissions" clearinghouse (keep track of which customers have given what permissions)
- Accelerate industry standards work in home energy management solutions (standards compliance and tests for interoperability)
    - There are a lot of components working together
- Synchronize various federal government agencies' (DOE, FTC, FCC, FERC, NIST, OSTP, etc.) activities on the topic—who is the lead agency?
    - All of these agencies have initiatives and reports
- Educating the federal government about the policies and regulations that states and local regulators have in place to address data privacy issues
- Issues such as who owns the data, who pays, and who has liability are not new. Maybe the definition of "data" is different, but the basics are already in place. The fact that it's not at the federal level may concern some in the federal government, but may not be a problem at the local level

Advantages, Disadvantages and Next Steps of a National Data Privacy Strategy

The breakout groups also discussed the advantages, disadvantages, and next steps of developing a national strategy to address privacy issues and activities. Participants agreed that there is a role for the federal government in helping to facilitate issues and solutions related to consumer data privacy. There was agreement that the desired method was not a national strategy, but rather a national approach that would provide leadership and a framework for the issues. A majority of the groups highlighted the need for the federal government to provide guidelines or a voluntary system, as opposed to mandates. One vision was for a high-level framework that increases uniformity across states without being too prescriptive.

Participants also noted that a national effort should prioritize consumer education. Consumers need to not only have a firm understanding of the concept of consent, but also an understanding of the value of electricity consumption data and the need for grid modernization. One suggestion was to make federal funding available to states in order to support consumer education on a local level.

Attendees mentioned the need for more transparency in the White House's "Bill of Rights," which will be released by the U.S. Department of Commerce and was noted by Ari Schwartz in his summary of activities. They noted that the "Bill of Rights" should also be more stakeholder-driven and include a single portal or lead agency for stakeholders to ask questions and provide inputs. Table 2 summarizes the thoughts on a national strategy as reported by the breakout sessions.

Table 2. Next Steps to Developing a National Strategy as Identified by Each Breakout Group				
Group 1	**Group 2**	**Group 3**	**Group 4**	**Group 5**
• Lead; don't command. **No federal mandates**. • Don't underestimate the **value of being a convener**. More meetings like today would be good. • Don't discount the value to state regulators of **developing models**. Lead by providing good ideas. Get these ideas out to the commissions and others to look at and evaluate. • Need to educate consumers	• Consider all stakeholders • Voluntary: no federal mandates • Map data as it moves. Where are the vulnerabilities? Clearly articulate handoffs • Leverage what other industries have done	• **High level framework** so that it helps increase uniformity across the states **but not too prescriptive** • **Form two collaboratives** for consumer protection • Policy: DOE and FERC collaborate on the policy and framework level • Consumer Issues: Consumer advocates, FTC, and others collaborate on consumer issues	• National strategy good but it shouldn't be overly burdensome. • **Leverage work** that is already being done. • Take inventory of work being done • Feel DOE is the most appropriate agency • Collaborate with local agencies that work with consumers on the street level • **Educate Consumers**: What are the value propositions? Need to explain the importance of modernizing the grid. Need to communicate the benefits (OMS, etc). When educating, don' t lead with privacy issue	• Accelerate cyber/ interoperability standards, including more outreach to states. • Make federal funding available to states to support consumer education on a local level. • **Let states** proceed to address business practices, including informed consent. • **Make the White House "Bill of Rights" stakeholder-driven** and more transparent, with a single portal/lead agency for stakeholders to ask questions and provide inputs.

APPENDIX 1: FINAL PARTICIPANT LIST

Eric Ackerman
Edison Electric Institute

Charlie Acquard
National Association of State Utility Consumer Advocates

Drew Bennet
Department of Commerce, International Trade Administration

Ron Binz
Public Policy Consulting

Tanya Brewer
National Institute of Standards and Technology

Steve Bossart
National Energy Technology Laboratory

Michael Brady
Comcast

Liz Burdock
Dow Lohnes Government Strategies

Ann Cavoukian
Information and Privacy Commissioners Office, Ontario, Canada

Paula Carmody
Office of the People's Counsel, Maryland

Scott Dailard
Dow Lohnes PLLC

Marti T. Doneghy
AARP/GRA Livable Communities

Dianne Dusman
Pennsylvania Office of Consumer Advocate

Patty Durand
Smart Grid Consumer Collaborative

Jeff Dygert
AT&T

Robert Fairey
Cox

Aryeh Fishman
Edison Electric Institute

Dan Francis
American Electric Power

Matthew Futch
IBM

Arkadi Gerney
OPower

Orijit Ghoshal
Citizens Utility Board

Ed Gray
Elster

Steve Hauser
National Renewable Energy Laboratory

Lizardo Hernandez
LandisGyr

Megan Hertzler
XCEL Energy

Retha Hunsicker
Duke Energy

Chris Irwin
U.S. Department of Energy

Cindy Jacobs
Environmental Protection Agency

Hank Kenchington
U.S. Department of Energy

Rick Kessler
Dow Lohnes Government Strategies

Kevin Lauckner
Honeywell

Roy Lathrop
National Cable & Telecommunications Association

Irene Leech
Consumer Federation of America

Michael Li
U.S. Department of Energy

Eric Lightner
U.S. Department of Energy

Robin Lunt
National Association of Regulatory Utility Commissioners

Peter McCabe
Wireless Glue

John McDonald
GE Digital Energy

Jeff McNeal
CoServ

Matthew Mansfield
Maryland Public Service Commission

Diane Moody
American Public Power Association

Jim Morozzi
GridWise Alliance

Susan Neel
CenterPoint Energy

Mike Oldak
Utilities Telecom Council

Ray Palmer
Federal Energy Regulatory Commission

Sunil Pancholi
Pepco Holdings, Inc.

Larry Plumb
Verizon

Jules Polonetsky
Future of Privacy Forum

Loretta Polk
National Cable & Telecommunications Association

Michael Pryor
Dow Lohnes PLLC

Ted Reguly
San Diego Gas & Electric

Ari Schwartz
U.S. Department of Commerce

Mary Ann Ralls
National Rural Electric Cooperative Association

Jim Reiley
PECO Energy Company

Ken Salomon
Dow Lohnes PLLC

Paul Schomburg
Panasonic

Stacia Sims
CoServ

Nick Sinai
White House Office of Science and Technology Policy

Anan Sokker
Florida Power & Light Company

Amanda Stallings
Public Utilities Commission of Ohio

Brent Struthers
Neustar, Inc.

Marianne Swanson
National Institute of Standards and Technology

Olivia Wein
National Consumer Law Center

Daniel Weitzner
White House Office of Science and Technology Policy

Jim Williams
Ohio Consumers' Counsel

David Wollman
National Institute of Standards and Technology

Ruth Yodaiken
Federal Trade Commission

Facilitation Team

Howard Andres
Energetics Incorporated

Tanya Burns
Energetics Incorporated

Tenley Dalstrom
Energetics Incorporated

Fred Hansen
Energetics Incorporated

Brian Marchionini
Energetics Incorporated

Rebecca Massello
Energetics Incorporated

Shawna McQueen
Energetics Incorporated

Katie Jereza
Energetics Incorporated

Rich Scheer
Scheer Ventures LLC

Samantha Solomon
Energetics Incorporated

Dylan Waugh
Energetics Incorporated

APPENDIX 2: AGENDA

Tuesday, January 31, 2012 • 8:30 am – 4:30 pm
Dow Lohnes PLLC
1200 New Hampshire Avenue NW • Washington, DC

8:15 am	**Registration and Coffee**
8:30 am	**Welcome** **Rick Kessler, President, Dow Lohnes Government Strategies** **Eric Lightner, Director, Federal Smart Grid Task Force, U.S. Department of Energy**
8:40 am	**Opening Remarks**
	Daniel Weitzner, Deputy CTO for Internet Policy, White House Office of Science and Technology Policy
8:50 am	**Participant Introductions**
9:15 am	**Summary of Ongoing Activities**
	■ Establishing a Framework for Third Party Access to Consumer-Specific Energy-Use Data, *Michael Pryor, Dow Lohnes PLLC* ■ **NIST Smart Grid Interoperability Panel Activities**, Marianne Swanson, Senior Advisor for Information System Security National Institute of Standards and Technology ■ **Green Button Initiative,** Dave Wollman, Deputy Director, Smart Grid and Cyber-Physical Systems Program Office and Manager, Smart Grid Standards and Research, National Institute of Standards and Technology Engineering Lab ■ **Department of Commerce Activities**, Ari Schwartz, Senior Internet Policy Advisor for the NIST Information Technology Laboratory, U.S. Department of Commerce ■ **Future of Privacy Forum**, Jules Polonetsky, Director and Co-Chair, Future of Privacy Forum ■ **State Energy Efficiency Action Network**, Michael Li, Special Advisor for Electricity Policy, Office of the Secretary, U.S. Department of Energy ■ **NARUC Activities,** Robin J. Lunt, Assistant General Counsel, National Association of Regulatory Utility Commissioners
10:15 am	**Break**
10:30 am	**Discussion of Value and Need for Energy Consumption Data – Breakout Groups**
	■ ***Focus Questions:*** What is the value of the electricity data provided by smart grid technologies to consumers? To utilities? What is the benefit of making the data available to consumers or their authorized third parties?
11:15 am	**Discussion and Identification of Key Issues – Breakout Groups**
	■ ***Focus Questions:*** What are the key unresolved issues surrounding smart grid data privacy (e.g., behavior tracking/surveillance, third party access, informed consumer consent, etc.)? What activities are underway to address each issue? Which issues could benefit from coordination and leadership at the national level?
12:30 pm	**Working Lunch – Hosted by Dow Lohnes PLLC**
1:00 pm	**Identify Possible Mechanisms and Next Steps for Addressing Key Issues – Breakout Groups**
	■ ***Focus Questions:*** How can current activities be leveraged or coordinated to help address the key issues? What additional activities are needed to address the key issues? What are the immediate next steps to begin addressing the key issues?
2:15 pm	**Break**
2:35 pm	**Report out from Break out Groups and Audience Q&A**
3:35 pm	**Next Steps for Developing a National Strategy – Audience Discussion**
	■ Review/revise proposed immediate next steps to begin addressing the key issues
4:15 pm	**Wrap Up**
4:25 pm	**Closing Remarks**
	Scott Dailard, Member, *Dow Lohnes PLLC*
4:30 pm	**Meeting Adjourns**
4:30 – 5:30 pm	**Happy Hour On Site Hosted by Dow Lohnes PLLC**

APPENDIX 3. BREAKOUT SESSION DISCUSSION OUTPUT TABLES

Breakout Session 1: The Value and Need for Energy Consumption Data

Focus Question: What are the reasons for providing consumers and third party access or not providing access to consumer electricity consumption data?

GROUP 1

Reasons To Provide Access	Reasons Not To Provide Access

• Basis for services
  - benefit to end user (vendor)
• Energy efficiency (industry)
  - to reduce cost and manage use benefits consumer and society
• To allow consumer to correct inaccurate information (industry)
• Enhance consumer conservation efforts consumer and societal benefits (state)
• Access can help consumers and companies conserve (industry)
  - energy efficiency and resource management
• Utility can use information to improve reliability and restoration (industry)
• Do provide granular data from meter (little to no cost) (vendor)
• Data in retrospect is what is most helpful to utilities (industry)
• The reason to provide data enables generation suppliers to tailor offers and fosters competition (consumer)
• The information might allow app developers to develop better tools and greater innovation (EPA govt)
	• Cost concerns for utility with provision of non standard data (industry)
	• If the burden is put on the utility to provide information, cost of managing privacy (industry)
	• Regulated concerns differ from those of non-regulated (industry)
	• Fundamentally, customers are required to provide information to begin with, and they should be able to control that information (consumer)
	• The information that is personally identifiable could fall into the hands of wrong doers who might stalk, break into homes, etc. (consumer)
	• Do not provide granular data from back office (costly) (vendor)
	• Customers are concerned about real time data being hacked/available (industry)
	• Increased risk of cyber attack on utilities (vendor)
	• Costs to utilities come back as a cost to the consumer/end users (industry)
	  - rate case
	• Could be a cost to the third party if the utilities charge for the third party service provider (state)
	• The concerns that we are raising are small in the big picture (industry)
	  - if the customers can save through efficiencies in supply cost, it could be huge

GROUP 2

Reasons To Provide Access	Reasons Not To Provide Access

• Inform the consumer to achieve a broad set of outcomes, examples include:
  - Enable consumer participation in smart grid activities such as:
  ▪ Demand response
  ▪ Energy efficiency
  - Increase consumer's understanding of smart grid value and achieve consumer satisfaction
• Measure carbon emissions from consumer electricity use
  - Aggregate other environmental impact totals
• Develop new features and/or products that add value to products already used in the home
  - With the consumer's permission, the data can enable solution providers to develop products that enable the consumer to find easier ways to reduce energy
• Extend telehealth medicine capabilities to more consumers and potentially create new capabilities
  - According to different levels of home energy usage
• Provide fine data for diagnostics, coaching to third parties, as well as to spur innovation
• Reduce emissions and the need for power plants
• Fair data practices
  - Demystify practices and comply with the law
	• Fear of misuse
	  - When the consumer is not sure of what the data will be used for, the natural response is to prevent access to avoid bad actors from using the data to cause harm or avoid actors who think they are doing a good thing from misrepresenting the data and actually causing harm
	• Non-consent shaming
	  - While municipalities want to showcase energy efficient people as an example of model neighbors that others should follow, they are actually raising red flags of bad neighbors who feel they are being unfairly mistreated
	  - Example: Gainesville, FL posts red, yellow, and green areas of energy usage on the internet; the way the information is displayed is offensive rather than motivating; comparing one neighbor against neighbor another creates tension rather than fostering "friendly competition"
	  - People should have the choice to not only make their usage information public, but also on how their information is communicated to others

GROUP 3

Reasons To Provide Access	Reasons Not To Provide Access

• 15 minute usage data can be provided to the Independent System Operators (ISOs) to be used for wholesale settlement without consumer expressed consent
• Consumers have the potential to save energy and money, provided that they are engaged and knowledgeable
  - Allows them to make informed energy decisions and save money on their bills, if they choose to do so
• Data can be used for academic and research purposes
  - Without the data, research is very limited in what it can provide
• Allows vendors and suppliers the visibility of consumption and usage patterns in order to better tailor their products to customer needs
• Law enforcement with proper documents (e.g. warrant or court order) can have access to the data in order to protect against criminal activity
• More accurate load data provides utilities with the ability to do upgrades and provide better service
  - Utilities can know which customers may be effected by an outage and provide priority restoration of services
  - Data can be used to prioritize curtailment
• Allows for reactive, instead of proactive, energy management for customers and third parties
  - Can be used for demand-side management, the development of new products, or making a business case
• Non-utility 3rd parties can use the data to develop innovative services, tools, and applications (e.g. dashboards to assist consumers)
• Mortgage industry can use the data to build energy efficiency into the assessment of a home's value
• Operations and maintenance oversight for data collection process
• Data can be provided to real-estate agents to help sell the home
  - Will know the homes average energy usage
	• Data could be provided to marketers that do not have consumer authorization
	• Providing the data could invade privacy or be used for unintended purposes
	• Can result in home security issues
	  - Provides the ability to know when customers are not in the home and creates general privacy concerns
	• Consumption data could be used for criminal purposes and to gain political advantage
	• Challenging to balance between cost and the responsibility of the data
	  - Granularity of the data
	• Marketing opportunity for curtailment service providers and representatives

GROUP 4

Reasons To Provide Access	Reasons Not To Provide Access

• Helps utility operations (load data)
• Enables energy management automation for improved energy efficiency and demand response
• Reduces peak load
• Motivates energy conservation practices (i.e., the Prius effect)
• Enables integration of renewable power and energy storage in local homes and businesses
• Enables real-time energy management products/services for the consumer
• Enables real-time pricing
• Allows consumers to reduce energy use
• Creates potential benefits or applications that are unknown at this time
• Manages peak load incidents
• Provides information to facilitate private investment in cost-reduction applications/technologies
• Allows for deregulated retail markets
• Creates a mechanism for dynamic pricing
• Allows for more accurate billing and more consumer control of usage
• Creates new products and services customers may like
• Empowers consumers by helping them understand what they spend their electricity money on
• Aligns wholesale and retail energy prices
	• Allows for unwanted marketing to consumers
	• Lacks funding for rule enforcement
	• Difficulties establishing price as different sector prices differ by utility (residential, industrial, commercial)
	• Even if utility liability for third party release of information is limited, improper releases will have negative impact on the utilities' image
	• Risks uninformed participation if customers are automatically opted-in; customers may not be aware of benefits and risks
	• Managing equity issues associated with different demographic groups
	• Potential that consumers are too busy to focus on this
	• Potential that the consumer does not want to spend time this way
	• Consequences of violating third party agreements are undefined
	• Inability to control the release of data beyond the third party
	• Lack of a need for home/building energy management systems to access utility data to be effective for demand response
	• Difficulty flowing responsibility with the benefits
	• Possibility of it becoming a reporting or compliance nightmare
	• Inability for utilities serving small (few customers), mountainous, large service areas to afford it
	• Misuse of information
	• Cost of managing large amounts of data
	• The upfront cost to the consumer might not be worth the benefits, especially limited/low income customers
	• Concern from consumers about who is using the data/for what purpose/will it be used against me or somehow to their detriment
	• Risks of data security breaches may increase if access rules are not carefully tailored
	• Concerns of "big brother" (e.g., tracking movement, pot farms)
	• Questions on the responsibility of third parties
	  - Post bond?
	  - Regulated utilities are clearly liable
	• Potential security risk (e.g., if hackers can tell when residents are not home)
	• Possibility that a fully competitive market is not the right thing
	• Possibility that consumers do not want usage shared with third parties
	• Results in less electric sales for utility

GROUP 5

Reasons To Provide Access

- For customers to understand and rationalize consumption patterns and behavior
- Interval consumption data helps consumers make decisions about their usage
- Ability to manage energy usage
- Facilitates and encourages energy conservation by consumers
- The key to effectively managing any scarce resource lies in measurement. Consumer electricity data provides the measurement capability
- Utilities need to share data with contractors who provide utility services such as data collection, management, and billing
- Measurement of performance of energy efficiency measures
  - As opposed to just predicting that the measures will achieve savings—this will help us actually verify those claims
- For the utility to be able to make its energy choices/usage more efficient
  - It can help the utility operate distribution networks more efficiently and avoid distribution upgrade costs

Other Points

- Consumers need to be able to determine if and what information they wish to share with third parties
  - Consumers need to know what's available in order to determine if they want to share it or not
- How do we know whose data it is?
- Fears about disclosure and potential invasion of privacy can undermine the value of smart grid
- This is creating a backlash against the advanced metering aspects of grid modernization. There are unsubstantiated, but real, consumer fears. CA, TX, and CO are really addressing this at a local level

Reasons Not To Provide Access

- Protecting the privacy rights of individuals
- Some consumers do not want their information shared
- Some consumers are concerned about third-party use of information
  - For unsolicited marketing/activities
- Ratepayers may be on the hook to pay for the costs related to the collection/storage/release of data
  - In a regulated arena, ratepayers pay for everyone's big vision
- Invites the unwanted marketing of products and the unwanted creation of personal profiles
  - Liability for improper/unauthorized sharing of data is unclear
  - Consumers don't want the information out there—who would be liable for improper sharing?
  - Utilities hope this will be straightened out, but, for now, they think it is an issue
- The data can be detailed, complicated, and easy to misinterpret
  - Consumers will be overwhelmed if they don't understand all of the data. The utility industry does not have a strong track record of effective consumer engagement
  - If utilities don't provide the data in a useful format, there will be a backlash
  - Consumers might think the information will go to government and law enforcement agencies
  - However, vendors will make the data useful to consumers. That is their job
  - There are some distinctions between commercial, industrial, and residential usage data. Do residential customers need monthly usage data every year? There could be diminishing returns
- Opens unintended uses for data stored over time (e.g., divorce lawyers)
  - There are some legitimate legal consequences here. See the recent U.S. Supreme Court decision regarding GPS data. Someone is collecting and storing this data, for how long?
- Unintended consequences in use of data by government and other entities
- Depending on the type and content of data, this could present security concerns
  - Putting some of the cyber and physical vulnerabilities in the public domain could cause problems. This includes voltage (operational) data, though, and not consumption data
  - Utilities want voltage and outage detection data to maintain the grid
- Fourth Amendment concerns
- Aggregated data has value, but it also has concerns about privacy in comparison with others
  - Privacy concerns with reintegrating the data must be balanced with the value of consumers being able to compare the normative data
  - Non-meter devices also gather information. This data doesn't go to the utility. Who is regulating this?
- Liability—what happens if there is a physical problem caused by data equipment?
  - Usually the utility is liable, but who is liable if an accident occurs when a customer adds something?

Breakout Session 2: Key Smart Grid Privacy Issues

Focus Question: What are the most significant privacy issues in providing access to consumer electricity consumption data?

Voting Question: What are the 3 most important of these issues that must be resolved to ensure consumer trust and acceptance of smart grid technologies?

● number of utility votes; ● number consumer advocate votes; ● number of vendor votes; ● number of state votes

GROUP 1

Creating Market Balanced with Privacy ●●●●●●	Education ●●●●●●
• **Competitive neutrality – how is the data collected, used and disclosed – it should be the same (industry)** • • Crafting effective privacy rules without stifling the market (industry) • How do you find a balance between the cost to utilities and protecting the consumers? (vendor) • National market creation scope and scale – uniform rules across state and market (vendor) • Ability to have a coherent conversation with customer – you want to have one conversation with the customer rather than several data specific information (Netflix, internet searches, etc) (vendor) • Lack of uniform guidelines, state by state – a national level standard would be useful to utilities, once it is downloaded the data becomes customer data rather than utility data, customer has choice to share it with third party (industry) • Principles vs. prescription – how do you build flexibility in this? You can quickly fall out of synch with how customers engage (vendor)	• Repeat direct notice to customers periodically, continued ability to release or restrict data (govt.) • How do we educate the public? In some areas, there would be backlash if utility tried to educate, some if the state tried to educate. Keep specific stakeholder groups in mind (state) • Inform the person at the point of purchase, but you cannot cover all the bases at the front end (vendor) • Companies and third party supplies need to consider how different demographic groups get their information (websites, phone, mailing) enable the customers to act on their responsibility to control their data (consumer) • Opportunity to educate consumer regarding what information will be available, and what it will be used for (industry) Segmentation • How do you make privacy policies simple and transparent for consumers? (vendor) • Education seems to come back to customer segmentation, and tailoring message to each stakeholder group • Clarity of communication in education – how clear are you being with your customers regarding your policies, and you may have to use various modes of communication to achieve actual **informed** consent? (industry) • From consumers perspective, where privacy meets security. Informed consent, letting people know what information will be provided to whom (consumer)

Controlling "bad actors" ●●●●●	Others
• Third party adherence to privacy, and non-disclosure rules – related to trust (consumer) • Practices to protect privacy – trust – you have an expectation that the utility or third party will protect your information (can it be, and how will it be?) • Enforcement – how to police bad actors (vendor) • The inability to detect the misuse of information is one reason to not participate (consumer)	• Opt-in versus opt-out – customer has to take step to either participate, or refuse to participate (consumer) ●●● • Trust between utility and consumer, how to make it grow rather than decline (state) If customers do not know what information is being supplied to whom, that trust can crumble. Trust is valuable (if enough customers complain, someone will hear, media) ●● • Simplified process for customers to provide information to the third party. Customer data downloaded by customer; their data, their choice (industry) ●● • Protecting privacy while still encouraging grid modernization (reliability and resiliency (state) • • Why are law enforcement officials so interested in electricity data? (surveillance, search, seizure, arrests)(consumer) ● • There is an issue with search and seizure (industry) creating a situation of wanting to provide as little information as possible (industry) • Expectations of privacy (consumer) because that is a foundation, albeit not well defined (with technology changes, expectations can change, and there are competing views) (industry) • Who owns which data? The utilities own the aggregated data, customers own their own personal data. What is the definition of the data? • We have a duty to protect consumers, but also a duty to protect the fair market. How do you protect the consumer without over-regulating? (state) • How long will the data be out there? Pandora's box (industry) • Data retention – the longer you retain the data, greater liability (industry)

GROUP 2

Key Issues			

• **Consent Process** (6) ●●●●●●
  - What does the permission/'green button' look like?
  - Is there a clear process, with clear communication of the pros and cons?
  - Can consent be given online, mail, etc.?
  - What exactly is the consumer agreeing to when consent is given?
  - Who can ask, give and validate consent?
  - What is the appropriate consent process from a consumer standpoint?
• Duration of consent
  - What is the appropriate length of consent?
  - Interests differ and are not well understood among parties of interest (state/federal/utility) on records retentions
  - Is the default automatically to opt-in or out of services that involve privacy considerations?
  - How to determine the continuation of service if consent is revoked?
• Controls
  - What are the right controls for data use, collection, or action?
  - How to balance the interest of all stakeholders; utility serves as a gatekeeper?
  - Area networks (internet, energy) may spill over as appliances 'talk' to each other, so which is in control, and what if each has a different privacy policy?
• Validation Process
  - Who validates the data; what is the process?
• Complaint process
  - Who do you go to when you are unhappy with how your data is handled?
  - Where are the boundaries between industry and the federal and state governments?
  - If vendors ask for consent, they should handle complaints (e.g., call service centers)
	• How data is regulated/protected as it moves differs at the national and state levels (4) ●●●●
	• How to avoid patchwork (e.g., customized state approaches), with a clear distinction on what should be handled by national and state levels?
	• Hand-offs trigger different jurisdictions
	• Sometimes data is regulated, sometimes not
	• Who is enforcing the management and accountability of data as it moves (are there minimums?)
	• What is the state regulator's authority and responsibility over third parties (non-regulated entities)?
	• How to ensure security and privacy when boundaries are not defined?
	• How to balance risk and policy and make them in sync on various fronts?
	• Are all entities that get this info under the same privacy policies? (3) ●●●
	• Consumer-oriented approach varies among states, and the level of control on what consumers give control over also varies (1) ●
	• Some or all data can be released by a supplier, given consent, but how can one be sure of to whom the data is given?
	• Texas gives consumers the power to decide to whom to give data
	• Consumers should have the ability to revoke data; privacy standards
	• What is sufficiently anonymous?
	• What are the boundaries for identification/aggregation standards for data?
	• Colorado example of no less than 15 persons
		• Data's value depends on the perceived value (4) ●●●●
		• Market can help educate the value of the grid; 'education to sell a product'
		• Consumers do not see the value of sharing data
		• Consumer value of data depends on their perception of it in terms of benefits and risks
		• As consumers perceive greater value of data and what it can allow, there will greater acceptance and understanding in regards to privacy
		• Understanding of risk vs. resolution and benefit vs. resolution of coarse and fine data
		• What are the coarse and fine data pathways?
		• Increased perceived risk with fine data
		• Literacy and informed consent (1) ●
		• Education and outreach: consumers need to understand the information that is given to them
		• The credibility of the data release process is critical to earning trust
		• How do you trust that what is released will remain private?
		• Decisions are based on fear rather than articulating the real problem (lack of controls and choices)
		• Smart grid is coming, whether utilities install it or not
			• Affordability (1) ●
			• Keep a level playing field amongst varied income levels
			• Cost (1) ●
			• Who pays, who benefits, and what is the limit in access?
			• Should costs for something like customized reports be spread over the consumer base, even though not everyone receives the benefits?
			• Should utilities take on data processing service role as they 'slice and dice' data?
			• Where is the access point for obtaining data – the utility or meters?
			• What is in the lead, technology or policy?
			• Consumers don't have much access to smart appliances yet, but will policy dictate the lead for their adoption?
			• Following the money and who wins/loses to see how this informs privacy policy
			• Vendors and utilities have varying business models
			• Lack of flexibility
			• Difficultly in foreseeing future problems
			• Do not want to create unintended issues/future roadblocks
			• Tracking relevance - do not track unless it's really important (1) ●
			• Not easy for consumers to access data (1) ●

GROUP 3

Policy	Financial	Third Party Access
• Consent for opt-in/opt out ●●● - Letting the customer say yes or no to giving out their data • Importing and exporting data from one region to another ● - Consistent rules between regions and regulatory authorities needed	• **Cost of implementing** ●●●●●● - **Cost/benefit may not be worth it** - **Underlying infrastructure may be too expensive**	• **Third party usage of data once it's release** ●●●●● - **Utilities have no control once the data is release** • Legitimacy of third parties ●●●● - Privacy seal to avoid getting ripped off by "Bubba's Home Energy Management" • Data security ● - How third parties protect data and transfer data - How third parties avoid theft and data breaches

Consumer	Behavior Tracking/ Surveillance	Other
• **Customer education** ●●●●●● - **Making customers comfortable and confident enough to have their data released** • Potential business confidentiality issues (i.e. how much power a facility is or is not using)	• Personal habits and potential surveillance scenarios ● - Being able to interpret lifestyle habits from load use to appliances, showers, and other general patterns • Ability to control of appliances over the internet	• Safety concerns - Knowing when someone is home, and when they are gone • Consumers want to have freedom of choice - Pre-pay option on products • Target for curtailment • Lack of data retention standards - Some utilities hold on to the data for longer than others

GROUP 4

Policy	Legal	Technical	Financial
• **How can a utility use/share customer data without consent and which uses should require consent?** ●●● - Who bears the burden of consumer education? • What is informed consent? ● • Do customers have the right to opt-out of data collection? State by state? ● • National market for energy use data doesn't yet exist - Need to avoid balkanization of state systems ● • Cost of implementation and how stringent/rigid the standards are should be balanced • Some states have unbundled and others have not • What rights do consumers have for aggregated/ historical data? • How is data released? - Who provides data to third parties? • Utility versus consumer • Lack of liability of various industries, e.g., information technology companies	• **Who is responsible for oversight of third parties?** ●●● - **Who engaged?** - **State/federal?** - **Generic privacy protections might work to develop oversight of third parties, etc.** • Who is ultimately responsible for the integrity of the data? Are there legal implications if data is not accurate? (cross-cutting with policy) ● • Define penalties for inappropriate release, jurisdiction for enforcement ● • Lack of a definition for personally identifiable information (PII) ● • What can the data be used for? - Credit card data is not just used for credit (i.e., used for auto insurance); is this to be expected? (cross-cutting with policy) • Who is responsible for managing consent? (customer relationships change) • Who pays if the customer experiences losses?	• **Lack of standards forcing mechanism for third parties and utility companies to ensure interoperability on a national basis (cross-cutting with policy)** ●●●● • Who are the different types of segmented data disclosed to? (cross-cutting) • Need to credibly measure the energy-efficiency benefits of smart grid and its associated services (cross-cutting with financial) • Technical capability to track the release of data (intentional and unintentional) - Traceability (cross-cutting with policy) • Delay in Smart Energy Profile 2.0 standard adoption	• Who pays and who benefits? ●● • Cost to utility to share data to third parties

Risk	Consumer	Behavior Tracking/ Surveillance
• **What is the Fear?** ●●● - **i.e., what is the risk/problem?** - **Who bears the responsibility?** • Opportunities for fraud • Lack of a track record in using consumer data (particularly residential)	• Very difficult to reach or educate customers in a way that effectively defines the value propositions ●●●● Customers will not support smart grid investment unless its value is communicated and delivered directly to the customer • Customers have had bad experience with other areas/ industries using data improperly ● • Concern that "big brother" will control personal energy use ● • Unintended use of data (good and bad) • Right to privacy, including energy • Managing the consent lifecycle (cross-cutting with technical and policy) • How are customers informed and how do we ensure informed consent? (cross-cutting with policy)	• Government could/would compel the utility or third party to turn over consumer data in the name of Homeland Security or the Patriot Act; consumers could lose control and their data could be used against them • Who/what entities have access to the data and will they use it against the consumer • Remotely tell if a customer is not at home

GROUP 5

Consumer Concerns	Government Jurisdiction	Data and Data Flows
• **Need for protocols and regulations for ensuring informed (i.e., affirmative) consent of the consumer prior to release to third parties** ●●●●●● - **Ensuring meaningful consent** - **Informed consent for third-party access** - **Cabining usage of data to consented uses** - **What are third parties? CO and CA have separated third parties (some want to help consumers with their energy usage)** • **Communicating with and educating consumers** ●●●●● • Lack of trust that data will be used for the (limited) purpose promised • Proprietary business data—potential for competitive harm - This is business privacy issue • Value to consumer—if consumer receives value from application and data, is privacy really an issue? - e.g., Amazon.com • Lack of common understanding about privacy practices/ protections - Fair Information Practice? - e.g., what the disclosures will get you, who is holding it, etc.	• Federal versus state jurisdictional oversight/areas of rights/responsibilities ●●● - The federal government has oversight on cyber security and interoperability, but states regulate local business practices and retail electricity sales • Rationalization/ synchronization of the multitude of legislative/regulatory/ voluntary standards ●● - There are different standards in different states • Industry standards—There are no industry standards yet from the NIST Smart Grid Interoperability Panel catalog of standards requiring privacy to be applied/incorporated • Third-party registration/ requirements oversight and jurisdictional reach of regulators - Private parties can do what they want, as long as they don't violate laws, but some states say they have jurisdiction	• Determining if data should flow directly from the utility to third parties (rather than access overseen directly by customers) ● - Why is the utility in the middle? • What is the scope of the data? ● - There is a big difference between consumption data and distribution optimization data - At what interval? Daily, weekly, or monthly data is different from hourly, 15-minute, or minute-by-minute interval data - There is also demographic profile data, billing and collection data, etc. - There are still privacy concerns with distribution optimization data • Does private data at some point become public? - How long should the utility keep the data? • Privacy in transit versus privacy at rest - Consumers can give access to utilities to share their data, but hackers could get the data while it's being transmitted • Meter/system constraints - What can we get out of the meters? What should utilities be required to monitor? In CO, if the utilities own the equipment, standards/policies apply. If they don't own it, they don't have to include it with advanced metering infrastructure • Opposing agendas or interests within industry - There are no common goals

Legal	Security
• What are consumers' rights to their own data? ● • Who pays for technology/program upgrades to ensure privacy? • Liability over improper/ unauthorized transfer of data • Does the fact that industry is heavily regulated or a government utility affect the expectation of privacy of data/personal information? - For municipal utilities, the utility is a government entity—what rights do they have to utilize the data for other purposes? - e.g., a small town might own a utility. What can the town do with the data? Who defines that? Who regulates that? How is it paid for? - There are different rules for government units to release information to third parties without informed consent • How much, what form, who pays? Freedom of Information Act versus warrant for data	• **Security of data transfers (between the consumer, utility, and third party)** ●●●● - Hacking, breaches • Data granularity—can the data be identified for a specific consumer? ●●● - Reintegration - Once the utilities get the energy/web data, will the databases be reintegrated so that they provide a clear picture of things that should be private? - If not, is privacy really an issue? • When to attack, when to rob - This is a consumer fear

Breakout Session 3: Possible Mechanisms and Activities for Addressing the Issues

Focus Question: What activities are needed to address the issues?

GROUP 1

Education	Guidelines	Customer Owns Data	Rate Structure	Other
• We need an education campaign on smart energy use; why you should care (aka smart grid capabilities) (industry) • Create education collaborative (consumer groups utilities third parties state regulators) (state) • Customer education focused on benefits, show them the purpose (industry) • Education for everyone (industry) • Thoughtful study of issues (facts on tech, existing policies, policy goals) (industry) • Understand motivations and interests of stakeholders (basis for consensus building) (industry) • Forums to share ideas/experiences/ solutions (industry) • Focus groups – ask consumers what they are looking for, what would make them use this, or not (state) • Document best practices (utilities, industries, and states) (state)	• Develop a seal program to implement voluntary enforceable codes on FIPs (fair information practices) via multi-stakeholder process(vendor) • Establish and maintain national standards for data sharing and communications (industry)	• Industry Button – give the data over to customers in a format that the customer can send it to a third party vendor, the utility is out of the equation (industry) - Relatively simple process - Reduces utility from liability of handling that data • The personally identified data belongs to the customer (consumer)	• Address rate structure and universal service issues (vendor) • Smart electric rates (time of use, dynamic pricing) critical to a market with electric vehicles (enabling) (industry)	• Consensus building – get buy-in (industry) • Principle before prescription (industry) • Encourage utilities to activate the capability of smart meters to communicate with HEMs (vendor) • Innovation more than educating people; you have to create a market, user interface matters (vendor) • Study the possible use of a “permissions” clearinghouse (keep track of which customers have given what permissions) (industry) • How do you structure this to balance out all of these interests? (industry)

GROUP 2

Potential Activities	

• Perform studies of approaches (privacy building blocks) and understand trade-offs
  - Research privacy policies that are already in place in other industries
  ▪ Understand why different sectors handle privacy differently
  ▪ States have different perspectives on privacy
• Perform scenario analyses
  - Walk through what concerns consumers
  - Are consumers getting what they want?
  - See what goes on at trade shows and state commissions (tech. vs. policy)
• Determine guiding principles and core benefits
  - Cascade to detail and prioritize
  - What is the vision?
  - Principles can be shared across utilities, etc.
• Use the privacy seal model
  - Crosses jurisdictional boundaries
	• Develop privacy policy that defines who is responsible after data leaves a utility
	  - State PUCs regulate utilities, so who is responsible after the utility?
	  - If the consumer has the data, what are the rules?
	• Privacy policy should cover data, not just smart grid data
	• Map data paths
	  - Involves multi-stakeholders
	• Define personally identifiable information
	• Determine significance of form factors/medium for collecting information
	  - Does the consumer care about the hardware that collects data?
	  - What are the issues surrounding the actual energy usage data
	• Promote smart grid by promoting education about where/how data is going to be shared
	• Develop standards (can come from anywhere (tariffs, rulemakings))
	  - Easier to deal with one consistent process than multiple ones across states, etc.

GROUP 3

Activities

• Develop a mechanism for consumer to file a complaint with breach of data
• Develop a certification process to verify customer authorization
  - Can establish a point of contact
  - Can allow consumers to trust that wrong parties won't have access to the data
• Develop a methodology for privacy by design to minimize rules and regulations for what you are trying to accomplish
• Have utilities and electricity service providers provide extensive, multi-faceted customer education programs and engagement
• Define a framework that allows states the flexibility to implement oversight
• Develop a national privacy policy that presents minimum protections, preserves PUC authority to implement, and establishes privacy certification for third parties that is not jurisdictional
• Mandate that the state commissions have cost recovery mechanisms to help utilities implement standards
• Utilities need to review their existing privacy policies and procedures, and update them as needed in relation to NAESB best practices and standards
• Continue to update privacy policies to accommodate new technologies
• Stakeholder can identify opt-out data fields and uses
• Develop rules and regulations to address control of the data by third parties
• Develop best practices for third party data
  - A standard for how those third parties deal with data if it is considered sensitive enough that it needs to be protected
• Certification and regulation of third parties
• Develop guidelines and rules for third party companies to transfer, receive, and secure data
• DOE should develop a comprehensive survey of existing privacy policies and practices in the states and utilities
  - State utility more comprehensive than what exists today
• DOE should provide forums for utilities and state rule makers to share information on solutions to customer problems
• DOE should talk to the Federal Communications Commission regarding customer choice and best practices
• Consumer education case studies
  - What has worked, what hasn't
• Customer education
  - Web and media campaigns that highlight the benefits to customers and utilities
  - Third party usage
  - NAESB Requirement 22 is a model
• Business practices guide

GROUP 4

Define What Needs to be Protected	Policies that Need to be Enacted	Customer Outreach

• What is personally identifiable information (PII)?
• Don't recreate the wheel, use or build on privacy standards and language that is already in place for telecommunications and the internet
• Use generic privacy protections
• Define the basic information that utilities need to provide safe, reliable service
  - Customer cannot opt out of providing this information to the utility
• Evaluate risk
	• Define roles and responsibilities of stakeholders
	• Decide whether this will be managed at the state level or federal level
	• Federal government could define baseline privacy protection requirements
	  - A consistent nationwide minimum that's communicated nationally
	• Build on established fair information and privacy standards
		• Define for the customer what data will be collected, how it will be used, and how it will be protected
		• Non-governmental organization or federal agencies should convey the messages to customers
		• Define value propositions for difficult customers
		• Messages should be easily understandable and come from a trusted party
		• Define the pros and cons of opting-in or opting-out
		• Benefits should be the leading message
		• Explain the importance of modernizing the grid

GROUP 5

Activities	

• Develop a national policy for defining customer-specific data; recommendations for informed consent procedures
• Synchronize various federal government agencies' (DOE, FTC, FCC, FERC, NIST, OSTP, etc.) activities on the topic—who is the lead agency?
  - All of these agencies have initiatives and reports
• Educating the federal government about the policies and regulations that states and local regulators have in place to address data privacy issues
  - Issues such as who owns the data, who pays, and who has liability are not new. Maybe the definition of "data" is different, but the basics are already in place. The fact that it's not at the federal level may concern some in the federal government, but may not be a problem at the local level
• Government as convener of an educational campaign. Engagement through social media and apps contests
  - Hopefully, demands for smart grid improvements will come from consumers wanting it. Consumers need someone to explain the value to them
• Flexible, provider-friendly privacy guidelines or protocols—not regulations or statutes
  - Vendors are concerned that there might be a lot of jurisdictional-specific rules and regulations that would make it hard to do business nationwide. What is needed is a nationwide privacy undertaking that has real enforcement without a comprehensive regulatory regime. (Regulations from the U.S. Department of Energy or the Federal Trade Commission are very prescriptive and too rigid. Regulations should accommodate different privacy tolerances.) Companies can commit to this undertaking, and receive a seal/icon that provides comfort to consumers
• Incorporate from other industries what they have done in terms of privacy and consumer engagement (e.g., banking, iPhone)
  - We can learn from their mistakes, e.g., no one understands banking privacy notices
  - The electric distribution industry is heavily regulated. It's a different model than even telecommunications, because consumers only have one option
  - People used to be afraid of putting their credit card information on the internet
  - There is a federal law that limits consumers' exposure to credit card fraud. But is there a comparable backstop for electricity consumption data? This could lead to problems. For example, a landlord could look at usage profiles when choosing tenants
  - There is case law about who gets data, when they get it, etc. For example, a sheriff could see lots of energy use in a home and think the homeowner is growing illegal drugs, but the sheriff would still have to obtain a warrant
  - This is not necessarily a new challenge. Browser and internet use data are comparisons. Companies and courts have figured out how that data can and should be released
	• Industry events to openly share best practices and lessons learned in consumer engagement and technology deployment
	• Clear rules of the road would make it easier to raise consumer awareness. We need more than just voluntary practices
	• Explain value to consumers!
	  - e.g., cell phones have significant radio frequency radiation and privacy concerns, but customers see the value of the product. Smart grid privacy issues will go away when customers see the real value of smart meters. Otherwise, there will be pushback
	• Define security standards for data transit
	• Accelerate industry standards work in home energy management solutions (standards compliance and tests for interoperability)
	  - There are a lot of components working together
	• Data security—federal input/guidance/requirements are needed. There is a need for processes to integrate federal and state utility regulation in cyber security and interoperability. Feds are not doing effective outreach to state entities that don't have the time or resources to participate.
	  - There is a timing disconnect between the multiple groups on the federal level and the states where meters are being deployed. (For example, in MD, there are work groups looking at cyber security and privacy issues.) There is a need for a simpler process to integrate parallel federal and state processes in order to assist state efforts. States might not have the expertise, so the federal government can help
	• Determine the proper roles of the federal government and state governments (e.g., in regard to technical protocols, business rules)
	• For example, states defer to the federal government on technical protocols for cyber security and interoperability, but states take the lead on business rules and practices for retail electricity sales
	  - This is a role issue. Federal agencies have roles (oversight, regulation), and so do states
	  - Indeed, the federal government doesn't understand the full plan or fully appreciate what already exists on the state level
	• Informed consent—data release. This is a state issue in terms of regulations and utility protocols, which are needed. This could be encouraged at a national level, but it should come from the bottom instead of the top
	• Clear rules on data
	• The rules must be clear, and the customers have to buy in. It doesn't matter if it's state or federal

Breakout Session 4: Advantages, Disadvantages and Next Steps of a National Data Privacy Strategy

Focus Question: What are your thoughts (e.g., advantages, disadvantages, next steps) about the development of a national strategy to address the issues and activities?

GROUP 1

- Main Discussion Points
• We may not need a national standard, but a national strategy would be helpful. The federal govt. could provide a framework • How do we get the standardization? Get some of the consistency across, which would lower costs • I always bristle at the notion that FERC would know better than we do about what is needed. Congress has requested states to consider issues, and that might be a good approach. PURPA mandate (industry) • One of the fed aggravations was that states sometimes gave due consideration to issues, and sometimes not. The seal is a way to move the ball forward without a hard prescription or regulation from DC (industry) • I think guidelines are good, but leave it to the states to develop their own rules and regulations, feel free to hold my hand, but don't push me into the water. We are more equipped to deal with our constituents than the federal government. (state) • We don't want to be mandated to do these things, and the differences between rules on privacy from state to state are not going to prevent this from rolling out (consumer) • We think that it is helpful to have these types of forums, in the role of a convener, but a hard regulatory regime set up on a national basis is not something we would like to see (industry) • As a state agency, my job is to protect the consumer, and every state views that protection in a different manner • For those federal employees who are disappointed in the role of convener, don't underestimate the importance of that role (industry) • Have a regional organization (industry) • RU 22 NASBI process, industry has appreciated and done well with, there is a need and an interest in moving things forward, and there are avenues (EEI for example) (industry)

- - Federal role as convener
- - Voluntary Guidelines, not mandates
- - Don't discount model rules

GROUP 2

Advantages	Disadvantages	Key Messages

• Can leverage solutions that are less costly
  - States or market may not have the resources to handle the issue
• Can speed up consumer awareness and technology development
• Can create consistency across the system
• Can create a broader dialogue
• Can raise the profile of the privacy issue
• National standards may allow more penetration of privacy policies
• Economies-of-scale can benefit the entire effort
  - Smart grid awareness can be accelerated from products and hand-offs that are consistent across all levels
  - The profit motive drives industry to educate on privacy so that consumers will invest in their products
  - For utilities, more players advertising extra services can expand consumer knowledge
  - Adds the 'yum'/incentive to having a smart meter
	• Privacy may not be the top issue amongst the stack of issues
	  - May not be relevant yet as some wait to learn from others
	  - Some prefer to be followers in adopting new technologies rather than early adopters
	• Bringing in extraneous parties may encumber the process; some groups do not see the need to involve others in these issues besides the utilities
		• Rather than a 'national strategy,' a 'national approach' would be better terminology
		  - Needs to be voluntary; does not mean a pre-emption or an order
		  - Information and trade-offs need to be clearly articulated

GROUP 3

Advantages	Disadvantages	Next Steps

• Could provide consistent framework guidelines across states
  - Would address the gaps in jurisdiction and provide minimum standards
• Could cross areas that are not required by state commissions
• Gives the opportunity to consider best practices from an array of jurisdictions in development
• Gives states and industry general guidelines, but if it is too specific, it could be considered a disadvantage
• Could provide a minimum level of privacy, allowing everyone to know what the rules are and how they can help lower costs
  - Provides freedom and flexibility among utilities
• Could help coordinate federal government efforts
• Could allow multi-national companies to operate more easily (through harmonization)
	• Could be "regulatory limbo" where the minimum level of standards/guidelines are set so it is too difficult to achieve
	• Prescriptive policy on functions and technology would stall innovation
	  - Drives up the cost
	• Federal mandates can increase costs
	  - One size doesn't fit all
	• Cost of compliance and implementation
	  - Each state starts at a different place
	• Infrastructure and resources will vary from utility to utility
	  - Could impact the timing of implementation
		• Develop a national approach that should be high level enough to increase uniformity across states and companies that deal internationally
		• Form two collaboratives for consumer protection
		  - DOE and FERC collaborate on the policy and framework level
		  - Consumer advocate, FTC, and others collaborate on consumer issues
		• Collaborate with NAURUC, EEI, APPA, NRECA, and others on how to facilitate implementation of NAESB recommended practices
		  - Deal with regulatory policies
		• Identify appropriate areas for a national strategy
		  - Message for DOE: this is not a utility specific issue

GROUP 4

Advantages	Disadvantages	Next Steps

• Avoids balkanization
• Provides baseline functional requirements
• Leverages existing activities
• Uses Open Smart Grid (Open SG) and Open Automatic Data Exchange as a starting point
  - Design privacy into the application
• Spurs innovation
• Builds consumer confidence
• Aligns visions and understanding
• Creates economies of scale and builds the knowledge base of the workforce by providing common standards
	• Could be overly burdensome or costly to comply with
	  - This could stifle innovation
		• Leverage existing work: find out what work is out there and develop an inventory, e.g.:
		  - Federal Information Processing Standard
		  - Open SG
		  - Regulation 22
		  - Third party practices (National Institute of Standards and Technology [NIST])
		  - Consumer bill of rights
		  - Smart Grid Interoperability Panel (SGIP)
		• Include banking, telecommunications, internet, and information technology work in this area.
		• Decide who is going to take the lead
		  - Possibly the U.S. Department of Energy
		• Collaborate with local organizations that are trusted
		  - For example, how NIST developed SGIP

GROUP 5

What Should Be Done	What Should Not Be Done	Next Steps

• Public Utility Regulatory Policies Act (PURPA) standard on data privacy
• Accelerate standards on cyber, interoperability
  - This would move things forward on a national level
• Take steps to integrate technical standards on state levels (bridge gap to state work)
  - Particularly with technical/cyber security efforts on the federal level
  - Could use the PURPA standard
• Federal funding to states to support local education to consumers
  - It's hard to effectively convey a high-level, top-down message. It would be better to work from the bottom up
• Continue collaborative workshops. Continue supporting technical coordination among stakeholders
  - Get all stakeholders (National Association of State Utility Consumer Advocates, other consumer advocates, utilities, government) together on a set of standards. This kind of workshop is helpful in getting people on the same page
	• Don't deploy technologies until they are ready
	• Let states proceed on business practices
	  - If not broke, don't fix
	  - Informed consent
	  - Utilities have privacy policies and practices. While nothing is foolproof, these policies and practices have been working for a long time
	  - The privacy community would say that the utilities have an excellent reputation for keeping data secure
	• No federally regulated privacy initiative
	  - No privacy Czar, such as in Canada
	  - There might be a role for this
		• Have more transparency on the White House's "Bill of Rights"
		  - Needs to be more stakeholder driven; consider holding a workshop
		  - Make crystal clear the objectives, goals, and vision
		  - Create a constitution for the next steps forward, as well as a statement of privacy principles that a broad consensus of stakeholders agree on
		  - What input will stakeholders have in this "Bill of Rights"?
		  - It's unclear if this is an internet or electricity distribution bill
		• Develop a clearinghouse/inventory on federal privacy activities that is easier to use than what currently exists
		  - e.g., webpage
		  - It's hard to track all of these activities
		• Have a SINGLE portal for stakeholder questions and inputs to the federal government
		• Designate lead agency, show coordination

APPENDIX 4: DOCUMENT REFERENCE

U.S. Department of Energy

Report, *Data Access and Privacy Issues Related to Smart Grid Technologies:* http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf

National Institute of Standards and Technology (NIST)

NIST Internal Report (NISTIR) 7628 Volume 2 – *Guidelines for Smart Grid Cyber Security: Privacy and the Smart Grid*: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

The Green Button Initiative

Website: http://www.greenbuttondata.org/

Department of Commerce

Green Paper - *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, December 2010, http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf

White Paper - Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, February 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

The Future of Privacy Forum

Main webpage: http://www.futureofprivacy.org/

Smart Grid webpage: http://www.futureofprivacy.org/smart-grid/

SEE Action Network

Main webpage
http://www1.eere.energy.gov/seeaction/

Customer Information and Behavior Working Group webpage
http://www1.eere.energy.gov/seeaction/customer_info.html

Privacy by Design

Website: http://privacybydesign.ca/

SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation
http://www.ipc.on.ca/images/Resources/pbd-smartpriv-smartgrid.pdf

Privacy by Design, The 7 Foundational Principles
http://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf

Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid
http://www.ipc.on.ca/images/Resources/achieve-goldstnd.pdf

Operationalizing Privacy by Design: The Ontario Smart Grid Case Study
http://www.ipc.on.ca/images/Resources/pbd-ont-smartgrid-casestudy.pdf

California Public Utilities Commission

Smart Grid Webpage: http://www.cpuc.ca.gov/puc/energy/smartgrid

CPUC Adopts Rules to Protect the Privacy and Security of Customer Electricity Usage Data:
http://docs.cpuc.ca.gov/WORD_PDF/FINAL_DECISION/140369.pdf

Colorado Public Utilities Commission

Rulemaking - Smart-Grid Data Privacy Rules, 4 CCR 723-3
https://www.dora.state.co.us/pls/efi/EFI.Show_Docket?p_session_id=&p_docket_id=10R-799E

Ohio Public Utilities Commission

Review of the Consumer Privacy Protection Customer Data Access and Cyber Security Issues
http://dis.puc.state.oh.us/CaseRecord.aspx?CaseNo=11-0277

National Association of State Utility Consumer Advocates (NASUCA)

NASUCA Resolution 2011-08 Urging 37State and Federal Officials to Adopt Laws and Regulations Requiring Electric Utilities to Protect the Privacy Rights of Customers by Prohibiting Unauthorized Disclosure of Personal Information, Including Energy Usage Data, November 15, 2011
http://www.nasuca.org/archive/Privacy%20Res.%20Final%202011-8.doc