Response to U. S. Department of Energy's NBP RFI: Data Access

DTE Energy
Distribution Operations, SmartCurrents Standards
12 July 2010

I. Introduction

The following is DTE Energy's response to the Department of Energy's (DOE) Request for Information on the subject of *Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy*, published in the Federal Register on 11 May 2010.

DTE Energy is one of the nation's largest diversified energy companies. Headquartered in Detroit, Michigan, DTE Energy is involved in the development and management of energy-related businesses and services nationwide. Its largest operating units are Detroit Edison, an electric utility serving 2.1 million customers in Southeastern Michigan, and MichCon, a natural gas utility serving 1.2 million customers in Michigan. The DTE Energy portfolio also includes non-utility energy businesses operating in 26 states which focus on power and industrial projects, coal and gas midstream processes, unconventional gas production and energy trading.

DTE Energy is demonstrating its commitment to creating value for its customers and shareholders through its SmartCurrents[1] program, which will implement Smart Grid technology at all levels of its electrical and gas distribution systems. This $170 million initiative seeks to lower the long-term cost of energy for our customers while increasing system reliability and stimulating economic growth in the region.

II. Executive Summary

DTE Energy takes its responsibility to manage and secure customer information, such as energy and billing data, very seriously. We feel that customer-specific information collected by utilities should be available to the customer through authorized access. Additionally, customer information should be kept confidential. Regardless of what information a customer may choose to be disclosed to third-party service providers, DTE Energy believes utilities must continue to have access and control over the data in order to maintain safety and reliability and for the more general purpose of providing the best and most innovative services available in order to economically meet the needs of the customer. DTE Energy believes the ability of utilities to access, control and use this information for legitimate utility-related purposes should be in no way constrained.

[1] SmartCurrents is a registered service mark of DTE Energy Company.

Most electric utilities have policies to protect customer energy usage data established on the principle that such information must be kept confidential, absent customer authorization for its release. The development of the "Smart Grid" with the potential to identify more detailed individual customer energy usage data raises the importance of having clear policies addressing customer privacy and unauthorized access to customer energy usage data. Accordingly, the Edison Electric Institute (EEI) and its members are developing some some draft guidelines for industry communications regarding Smart Grid customer energy usage data. DTE Energy, along with several other utility companies, is participating in the development of these guidelines.

All services provided by DTE Energy's electric and gas utilities are regulated by the Michigan Public Service Commission. There are significant costs, potentially hundreds of millions of dollars, involved in deploying technology with real-time information capability. DTE Energy believes that there should be no mandate for utilities to implement new technologies and bear this significant cost burden or pass it on to customers, regardless if they choose to participate. Utilities must retain the ability to recover all costs involved and new service providers must take the responsibility to reimburse utilities for the cost of implementing their new services that require real-time information.

III. Responses

Question 1: Who owns energy consumption data?

As used herein, "Energy Consumption Data" is defined to mean **only** the amount of consumption of electricity and/or gas, as registered via the meter(s) provided by the utility, and includes **no** other information.

Energy Consumption Data does not exist until it is produced, meaning collected and compiled. Since Energy Consumption Data is produced by the utilities, it is owned by the utilities, but is provided by the utility to the customer in the normal course of business.

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

The term "energy information" does not appear to be a defined term, but should be defined so that all parties clearly understand its breadth.

The owner of the specific piece of Energy Information (as that term is used in these answers) should be entitled to privacy protections relating to that specific piece of Energy Information. For example, if a customer provides personal information to a utility, then that customer owns that personal information and the utility may only use that personal information for its allowed business purposes. If a utility obtains information from a third party, about a specific customer, or class of customers, then the third party will generally own that information and the utility may only use that information in accordance with the contractual terms under which that information was provided to the utility. Further, parties must also comply with applicable statutes that set forth additional, or different, privacy protections. DTE assumes that "Energy Information" will include personal information, Energy Consumption Data, utility-created information, as well as information that a utility may obtain from a third party(ies) related to the specific customer, or group of customers.

Some Energy Information will include utility proprietary information, which by its nature plays a key role in any business strategy and therefore will have actual or potential economic value. This includes business and marketing plans, sales and marketing data, and financial and operating data. Any proprietary information needs to be owned by the respective utility.

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

Privacy practices ("Policies") should be established by each respective utility to safeguard the confidentiality and security of Energy Information (as that term is used in answer #2), which includes customer records such as address, email addresses, phone numbers, energy consumption, payment histories, credit ratings, account numbers, identification information, etc.

These Policies should include who has access to Energy Information , under what circumstances, and also set forth access controls to limit access to such Energy Information. These Policies should include guidelines for the dissemination of such Energy Information to third parties or law enforcement investigations. These Policies may allow for the dissemination of such Energy Information to third parties that are under contract with the utility company, provided that Energy Information is used for performing services on behalf of the utility, its agents, or affiliates. This same provision applies to third parties operating under a formal agreement (or as governed by state or federal law) with the utility to exchange Energy Information and which include non-disclosure terms and conditions.

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

Customers should not be allowed to opt out of smart meter deployment. Utility business cases for investments in smart meter deployment are predicated on 100% deployments for their cost justification. If customers could opt out of smart meter deployment, it would decrease the overall benefits and increase the cost for all customers due to the inefficiencies of a partially automated metering system.

If a customer owns the specific Energy Information, then that customer should have control over that customer-owned portion of the Energy Information that is shared with third parties. Further, any Energy Information provided to a utility by a customer, may be used by that utility for any related utility purpose.

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

Utilities and their Public Service Commissions have implemented many safeguards for customers in regards to billing and service issues. To report concerns or problems with the smart meters, customers should be able to use the same reporting mechanisms that they would use for reporting any other type of service trouble or concern.

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

Policies and practices for utilizing and securing Energy Consumption Data should generally apply equally to all customers, but the utility should be allowed the flexibility to develop policies and practices that are unique for each community/group of customers it serves. Utilities should continue to utilize that data to optimize and maintain safety and reliability, while exploring cost efficient and innovative services to better serve the respective community/group of customers.

Question 7: ***Which, if any, international, Federal, or State data-privacy standards are most relevant to Smart-Grid development, deployment, and implementation?***

Any privacy standard, if it flows from any statute or regulation, would be relevant to Smart Grid development, deployment, and implementation. In addition to those, the following would likely be relevant to Smart Grid development, deployment and implementation:

- Michigan Public Service Commission Rules and Regulation governing electric and gas utilities
- Michigan's Identity Theft Protection Act
- FCRA (Fair Credit Reporting Act), including its amendments (FACTA, and Red Flags, etc)
- Michigan Social Security Number Privacy Act (SSNPA)

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

The following data privacy standards would be well suited to provide a framework to accommodate varying customer expectations:

- AICPA Generally Accepted Privacy Principles (GAPP)
  GAPP represents the AICPA and CICA contribution to aid organizations in maintaining the effective management of privacy risk, recognizing the needs of organizations, and reflecting the public interest. GAPP is to be used as an operational framework to help management address privacy in a manner that takes into consideration many local, national, or international requirements. The primary objective is to facilitate privacy compliance and effective privacy management. The secondary objective is to provide suitable criteria against which a privacy attestation engagement (usually referred to as a privacy audit) can be performed.
- Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
  The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980, continue to represent international consensus on general guidance concerning the collection and management of personal information. By setting out core principles, the guidelines play a major role in assisting governments, business and customer representatives in their efforts to protect privacy and personal data, and in obviating unnecessary restrictions to transborder data flows, both on and off line.

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

Educational materials can be made available to customers explaining the benefits and potential risks associated with allowing access to their energy information. When mechanisms are made available, the customer should be advised of such benefits and potential risks and require the customer's express consent to release such information to any third party. Third party companies should be required to provide clear and understandable information to consumers regarding the implications of using their services. As used herein, third party does not include a party acting as an agent, or under contract, for the respective utility.

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

Security architecture provisions that relate to cyber security and customer privacy should be implemented according to applicable standards, laws and corporate policies to prevent unauthorized access to Energy Information. Security architecture provisions must safeguard both privacy and integrity of Energy Information. Provisions should provide for comprehensive cyber security organizational capability and system infrastructure. Security architecture provisions must continually protect the confidentiality, integrity and availability of Energy Information as well as system and device data, ensure ongoing audit ability and event tracking, and ensure that robust response mechanisms exist to react to unknown or emerging threats. Specific aspects of security architecture provisions include time-date stamping (integrity/availability), data encryption (confidentiality), signed authorization (confidentiality) and network segmentation (integrity). Security assessments on products, software, devices, technologies or services, should be conducted both internally and externally. Smart grid infrastructure should remain isolated from communication technologies between third parties and the customer to preserve the security of utility operations to provide electrical service.

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

DOE can best implement its Smart Grid mission and duties by developing its recommendations that are in concert with existing laws and regulations, with deference to Policies (as that term is used in answer #3) developed by each utility.

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

Energy Consumption Data (as that terms is defined in answer #1) should only be provided to federal, state, or local governments in accordance with the established Policies (as that term is used in answer #3 above) and/or law or regulation. For example, governmental agencies are viewed as third parties and generally require the consent of the customer for release of customer specific data. Broad general data release is governed by state laws imposed on utilities for release of data to the

general public. These provisions have been time tested and proven to provide security to the electrical system and the customer.

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

Third parties should only have limited access to energy information under specific, written, and prescribed policies. These prescribed policies, including cost allocations and processes, need to be developed.

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

Billing rules already require that a customer be provided with energy usage information corresponding to their current bill as well as historical usage data. The Michigan Public Service Commission is also looking at other aspects of data availability. As Smart Grid capabilities evolve, it is anticipated that customers would be provided with data such as interval usage data, pricing information, demand response signals, and disconnect status.

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

Current Smart Grid technology pilots underway such as the ARRA grant projects, including DTE Energy's SmartCurrents[2] Project, and the Pacific Northwest Smart Grid Pilot, will help to provide a better understanding of the energy information that may be desired by customers. The pilots will also help identify the feasibility, costs, and security requirements associated with providing real and/or near real-time data to customers.

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

The Michigan Public Service Commission has implemented a collaborative process in which policies for Smart Grid privacy, data collection and third party use of information will be formulated.

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

DTE Energy has policies in place that address the privacy of customer information. These policies govern access to customer information by utility personnel and third parties. These policies allow for authorized access by a customer to his or her customer information. As part of ongoing continuous improvement efforts, all DTE Energy data privacy and security policies, including those

[2] SmartCurrents is a registered service mark of DTE Energy Company.

related to Smart Grid implementation, are continually being reviewed for potential enhancement, clarification or consolidation.

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

The existence of customer data policies that respect customer privacy and the proprietary nature of business information should be a legitimate part of the DOE's consideration when evaluating future Smart Grid grant applications.

IV. Conclusion

Utilities occupy a unique position in society. Our mission is to provide energy services that support basic living conditions for the people, businesses and institutions we serve. Our systems are completely tied to the geographic regions in which we operate. Our livelihood is based on building, maintaining and operating infrastructure to serve customers, who include ourselves, our families and our neighbors.

DTE Energy appreciates the opportunity to provide these comments on behalf of its customers and its shareholders for consideration by the Department of Energy.

Respectfully submitted,

DTE Energy Company

/s/ *William R Cloutier, Jr*
William R Cloutier, Jr
Manager, Distribution Operations, SmartCurrents Standards
One Energy Plaza, Room 381 WCB
Detroit, MI 48226
(313)235-8135
cloutierw@dteenergy.com

/s/ *Ronald W Vader*
Ronald W Vader
Engineer, Distribution Operations, SmartCurrents Standards
One Energy Plaza, Room 381 WCB
Detroit, MI 48226
(313)235-8509
vaderr@dteenergy.com