NBP RFI: Data Access
Honeywell Responses

To Request for Information (RFI) from the Department of Energy on Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy

1. Who owns energy consumption data?

The utility needs access to "raw" billing data, i.e., meter readings that take place every time the price changes and allow the utility to calculate the consumption during a particular time period and rate the consumption according to the price in effect during that period. Based on the FIPP principle of data minimization, it is expected that these meter readings would occur just a few times per day (e.g., every time a new price period begins under a ToU pricing scheme and every time a critical peak price event is put into effect); the measurements will be transmitted over an AMI network to the utility back-office. This data will be kept for purposes of billing, audit trail, bill explanation, etc. and should be shared only with the customer. This is no different from the way call detail data is handled by phone companies today or the way electric utilities handle monthly measurements today.

Smart meters have the ability to take readings at intervals as frequent as a minute or even a few seconds. This detailed consumption data is not needed by the utility but can be very useful to the consumer if provided in near real time (less than 10 seconds delay): the information can be displayed on in-home energy displays to help consumers understand their consumption patterns and how they can reduce it or shift it to off-peak hours. The information can also be fed into controllers / home energy managers that can take decisions automatically based on preferences programmed by the consumer, allowing the consumer to "set and forget."

The raw billing data and the detailed consumption data are very different in nature, although they both originate at the same device (smart meter). The detailed consumption data is much more voluminous (possibly by several orders of magnitude) and reflects a consumer's private life or business. The data is sensitive from a privacy and security standpoint. For example, energy consumption is a strong indicator of occupancy (or lack thereof, which may invite crime); would consumers want others to know when they are not at home or in the facility?

Thus, detailed consumption data needs to be owned by and be under the absolute control of the consumer. Besides, since consumers pay for the meters (through the rate base), consumers are entitled to the data generated from the meters.

The best way to make the detailed consumption data available to the consumer while preserving the consumer's privacy and ensuring the consumer's control over the data is to allow the smart meters to be read directly from equipment residing on the customer premises (in-home display, home energy manager, etc.) This architecture is also the most economically effective, since it removes the burden of data transmission and processing from the utility. Furthermore, the consumer is free to forward the data to a third party service provider if the consumer so chooses.

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

   The energy consumer is entitled to privacy protections, since (i) the consumer pays for the energy usage and the meter that measures it; (ii) the consumer owns the information regarding that usage; and (iii) the consumer's private activity is reflected in that usage.

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

   Privacy and security are best served by transmitting detailed consumption data directly from the meter into the customer premises. Any approach which moves detailed consumption data through networks outside of the premises or stores such data in remote locations incurs unnecessary privacy and security risks.

   The centralized storage of data (e.g., in an internet-based solution) makes the data susceptible to remote attacks. Furthermore, the consequences of a potential security breach in a centralized location can be much more serious: the compromise of a central location could lead to the loss of data from a large number of homes or facilities, which, in turn, could allow destabilization of the grid if all those homes or facilities were affected by the attacker.

   For data that needs to be stored in central servers (e.g., billing data mentioned in the answer to Question 1), the privacy and security practices employed (e.g., data encryption, authentication / access control) should be similar to those used for data of similar sensitivity (e.g., internet banking).

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?**

   Consumers should not be able to opt out of smart meter installation. These devices are part of utility modernization programs that help improve the electrical grid operations; in addition to generating consumption data, smart

meters typically allow remote connect / disconnect, provide fault information, etc. Furthermore, if a customer were allowed to opt out of smart meter installation, the utility would incur unnecessary expenses to maintain two different types of infrastructure or to install a meter at a later point in time when the occupant of the house or facility changes (it is far more economical to install smart meters across an entire neighborhood than to do it one customer at a time). These unnecessary expenses would be unfairly borne by other consumers.

However, consumers should be allowed to opt out of detailed consumption data, since such data should be entirely owned and controlled by consumers.

The collection and storage of billing data by the utility (as mentioned in the answer to Question 1) may also generate privacy concerns for some consumers, since such data may reveal some consumer activity (although not nearly to the degree revealed by the detailed consumption data). The issue can be resolved by allowing the consumer to forego detailed billing; the utility could simply maintain the accumulated account balance by rating the consumption during each period, adding the charge for the latest time period to the balance and discarding older measurements.

Consumers should have absolute control over the sharing of any usage related data (billing or detailed consumption). The default policy should be to disallow any kind of sharing unless the consumer explicitly elects to authorize sharing of the data with explicitly named parties.

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

Energy services providers (i.e., utilities) typically purchase and install smart meters without any direct input from the energy consumers. The utility uses the smart meter as an essential device for measuring the energy used by a facility and charges the owner of the facility (consumer) accordingly. Therefore, the energy services provider should be responsible for the complete and proper operation of the smart meter. If a consumer experiences a problem with the smart meter, the energy service provider that installed the meter should respond to the problem immediately through its customer service operation, which should be available to the consumer 24 hours a day, 365 days a year. In case the consumer experiences a problem with the customer service operation, the customer should also have other resources available to contact for help, including the state energy or utility commission.

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?**

   Low-income consumers are best served through innovation in the open market. Competition will ensure availability of better and cheaper products, just as has happened in other industries. For example, innovation and competition have made cell phones and cell phone services very affordable even to low-income consumers.

   If policy makers determine that low-income consumers need help to pay for new technologies, this help should come in the form of monetary subsidies (e.g., rebate coupons) for qualified products available in the open market or in the form of product procurement by the utility to those consumers (e.g., several utilities have programs that install efficiency measures free of charge to low-income consumers – the same could be done for smart grid devices). The consumers of new technologies should be the ones that decide which technologies are the winners. Therefore, public policy should encourage the open market in new technologies, which, in turn, will encourage innovation in new technologies. Put another way, government officials should not be choosing among competing technologies for consumers, including low-income consumers.

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

   Not Answered.

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?**

   Not Answered.

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?

Today, consumers enjoy an appropriate balance of strong data privacy and easy access to sensitive information. For example, consumers can access bank accounts from their cell phone and file taxes on the internet. These mechanisms are available and used today in many existing communications architectures and will continually improve over time to ensure that proper balance is maintained. The smart grid can take advantage of this by utilizing these existing communication mechanisms with little to no investment.

The access by third parties to a consumer's energy information should be at the absolute discretion and under the complete control of the consumer. The default should be that no access is granted by a utility to a third party unless the consumer explicitly authorizes such access and explicitly specifies the third party. Appropriate measures need to be put in place by utilities to protect consumers from practices like "slamming" (an unscrupulous practice common in the telephone industry – see http://www.fcc.gov/slamming/), "phishing," etc.

To accommodate a range of consumer preferences on the tradeoff between access and privacy, consumers should be allowed to specify the granularity (sampling rate) of the data provided to a third party. For example, below are the benefits as well as the data privacy risk for select intervals.

- 15 minute intervals:
    - Benefit – Allows a third party to analyze energy use patterns and recommend improvements.
    - Risk: This information allows an observer to determine when you wake up, when you leave for work, when you return and when you typically go to bed.
- Daily interval:
    - Benefit – Allows a third party to perform some analysis such as comparing consumption to previous days or comparing consumption with neighbors.
    - Risk – This information allows an observer to determine if the home is occupied or if you are away on vacation.
- Monthly interval;
    - Benefit – This allows a third party to make comparisons to encourage reduced consumption. E.g., you used 10% less this month than last month and 15% less than the same month last year.
    - Risk – very low.

By allowing consumers to specify the granularity of the data, each consumer will be able to choose a level of risk with which the consumer feels comfortable.

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

Interface for direct meter reading from customer premises. While this may not appear to be a data security measure on the surface, it is the provision that will have the most beneficial impact on protecting consumer privacy, because it will allow consumers to enjoy the benefits of very detailed (possibly at sub-minute intervals) consumption feedback in near real time (under 10 seconds delay) while eliminating all concerns about third party access to the data. This provision obviates the need for data collection and storage on remote servers and ensures that the data is in the possession of the consumer.

Meter firewall: The meter must implement a two way firewall function. This firewall will protect the utility from hostile activity originating in the home area network (HAN). The firewall will also protect the home area network from intrusion via the AMI network.

On-premises media access: The home area network (whether wireless or power line carrier) must employ cryptographic security mechanisms to:

1. Prevent eavesdropping on the data in the home area network.
2. Prevent attackers from gaining unauthorized access (penetration of) the home area network.

   If an attacker penetrates the home area network, they may disrupt operations in the home (e.g., shut down the furnace causing pipes to freeze). In many homes, the home area network (energy management network) will be connected to the home data network (home PC). Penetration of the home area network may provide an attacker access to the home PC/LAN behind the internet gateway/firewall.

Internet Gateway: If the home area network is connected to the home internet gateway/router, then the gateway/router must contain mechanisms to prevent ports opened for energy management traffic from compromising either the home area network (energy management) or the home data network (PC). For example, ports on the internet gateway/router may be opened to allow a third party to perform direct load control via the internet. Firewall and cryptographic mechanisms must be employed to prevent an attacker from gaining unauthorized access to the home area network or home data (PC) network via these open ports.

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

The DOE makes a very significant impact in the market place through the SGIG and SGDP grants. The substantial funds ($4B) infused in the market will have a significant direct and indirect impact on the architectures that will emerge. The direct impact will come from the devices (meters, in-home displays, smart thermostats) that will be deployed; these deployments will create a de facto architecture. Furthermore, since the early deployments will "seed" the market, there will be a significant indirect impact on future deployments even if they are not funded by DOE: utilities will prefer to deploy the same type of infrastructure across the rest of their territories.

Given the importance of the DOE smart grid grants, it is imperative that the evaluation by the DOE of future grant applications take into account data accessibility policies and ensure consumers are allowed direct access to their smart meters through standardized interfaces (see answer to Question 18).

The same considerations should be used to guide the deployments under the grants already awarded if contractually possible. At the very least, the DOE should request detailed reports from awardees explaining their approach to accessibility policies, current direct meter reading capabilities and provisions for upgrades to future standards, etc. Also, the DOE should highlight these issues in the Smart Grid Information Clearinghouse and provide higher "scores" for deployments that address availability and privacy of energy consumption information successfully. The Clearinghouse is likely to be used by utilities and policy makers at all levels (including states and PUCs) to make decisions about subsequent deployments, so the Clearinghouse is a great way to create awareness of these issues.

The DOE can also create awareness and promulgate best practices regarding privacy and standards for direct meter access through its other activities, like the national action plan on demand response on which the DOE will collaborate with the FERC. Furthermore, the DOE can organize seminars and develop informational materials for state regulators; these seminars can highlight the data accessibility and privacy issues, provide the lessons learnt from the smart grid deployments across the nation and recommend best practices.

Finally, the DOE should continue to provide guidance to NIST regarding the development of standards that take into account data accessibility policies.

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

Energy consumption data can reveal information about a consumer's activity (e.g., presence / occupancy, location and time from electric vehicle charging). This information can be sensitive in ways similar to other information (credit card data, banking transactions, telephone call detail records, etc.). Therefore, appropriate mechanisms need to be established for determining if, when and how government agents can get access to such information.

There is a well-established basis for how government agents can get access to similar data (banking records, credit card transactions, call detail records) and what data other types of utilities need to provide to authorities and when (e.g., CALEA for phone companies). The body of knowledge gained from these other industries can be used as the starting point to derive appropriate mechanisms for the electric utilities and the energy consumption data.

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 have access to private consumer energy usage information only if approved by the consumer.

Privacy standards / guidelines already exist for handling access to financial information, medical information, etc. These standards / guidelines should be used as a starting point for establishing standards / guidelines regarding energy information.

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

Consumers should have access to the interval measurements taken by the utility to calculate their bill under a variable pricing scheme (e.g., ToU with critical peak pricing). See response to Question 1.

Consumers should also have access to detailed facility consumption data in near real time (less than 10 seconds delay) and at intervals as frequent as the meter hardware allows. The primary method to provide such access should

be by direct reading of the smart meter from the customer premises. The detailed data will allow the consumers to observe the impact on aggregate consumption of running various loads (HVAC, water heater, pool pump, lights, appliances, etc.) and to also program control devices to take actions automatically based on the consumers' preferences ("set and forget").

If any other private energy usage information is available, the consumer should have access to it.

A third party should have access only to information which a consumer explicitly authorizes the third party to access.

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

Consumers should be allowed to read their smart meters directly from the customer premises in near real time (less than 10 seconds delay) and at intervals as frequent as allowed by modern smart meter hardware. Standardized meter interfaces should be created and enforced for such access, so that the free market can supply customer premises equipment (in-home displays, home energy managers / controllers, etc.) that enable direct meter reading. This is the best way to ensure that consumers derive the maximum benefit from the meters they are paying for while protecting their privacy. This approach also provides maximum flexibility with respect to access by third parties: if the consumer is in possession of the data, the consumer can decide what to do with it.

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

Not answered.

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?

Not answered.

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

The DOE should definitely consider consumer data accessibility policies when evaluating future Smart Grid grant applications. The consumers (and tax payers) are paying for the smart meters via rate increases and taxes. The DOE's evaluation criteria for future grant applications should dictate that consumers have full rights to near real time (less than 10 seconds delay) access to detailed energy information through direct meter reading from the customer premises.