Comments of Avista Corporation

(1) Who owns energy consumption data?

Utility customers consume electricity and gas minute by minute which is measured in kilowatt-hours aggregated for a period of time known as an interval. Certainly, customers have both an interest and a right to acquire their usage information. Whether that be information interval-by-interval or provided as an aggregation for the billing period. The trend in other industries is to provide more detailed usage information. The utility invests a great deal of money to install, maintain and operate the infrastructure that both measures and delivers gas and electric products to the customer. Consumption data is a necessary input for effective planning and operation of that infrastructure. The utility as the owner of the data has the obligation to maintain customer privacy.
At the present time Avista believes that a utility owns the energy consumption data collected by its meters since such data is a record kept in the normal course of business and the basis for billing and revenue collection. Furthermore such records, in the aggregate, are critical for the utility's ability to meet long range regional capacity demands. Another facet of the consumption data ownership question lies in the data breach statutes. According to the Consumer Data Breach statutes in most states (particularly in Washington, Oregon and Idaho) a business that collects and maintains computer records containing personal identification information associated with customer accounts is the "owner" of the data for purposes of data security and protection. As the "owner" of the information, the business is required by the statutes to provide notification to the customers whose account information has been compromised in a breach.

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

A nation-wide survey of federal and state case law in June 2010 shows that the majority of courts have held that there is no legitimate expectation of privacy in utility customer power consumption records, in the context of subpoenas and requests for records by law enforcement. These cases, however, predate the deployment of "smart" meters which go beyond the simple recording of electrical consumption on a month-to-month basis and may provide time of day usage and the power consumption of individual appliances on the Customer's side of the meter. The only constraint on the use of customer information under WUTC regulations is the prohibition on providing or selling such information to third parties for commercial purposes not related to services provided by the utility. Another consideration for commercial customers may be that protection of such data might be important for competitive reasons. Customer information gathered in connection with time-of-day metering and metering of appliance energy consumption should be protected from disclosure to utility affiliates and subsidiaries, and to third parties for commercial purposes.
Avista believes utility customers, as consumers of electricity and gas, warrant privacy protection that restricts access to consumption data to only those parties that consumed the product.

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

Key provisions should include:

- **Strict internal controls on utility employee access to and use of customer information and records;**
- **Strict controls regarding authentication/identification of customer with respect to electronic access to customer and consumption information.**
- **Prohibition on the release of individual customer energy information to third parties for commercial purposes not related to the services provided by the utility;**
- **To the extent that a utility uses third party service providers, under contract, to process individual customer account information (for such things as account maintenance, billing, payment via credit card or bank transactions, or usage display via the internet), the service contracts should contain strict non-disclosure provisions regarding utility customer account information protection provisions;**
- **Encryption of individual customer consumption information transmitted by smart meters to the utility and/or third party service providers;**
- **Policies for the controlled release of individual customer energy consumption information to law enforcement and other government or social service agencies;**
- **Annual reviews by utilities of data breach incidents reported by other utilities, technical vulnerabilities and enhanced data protection measures.**
- **Meters installed at customer premises should not store or transmit customer information. Access to meter contents should not be allowed without authentication between the meter and the monitoring device. This implies the utility must register monitoring devices at least until such time that meters provide multiple levels of user/password access.**

(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?

Utility consumers should not be able to opt out of smart meter deployments. Smart meters installed as a part of an overall AMI system, collectively create the infrastructure necessary to achieve operational benefits and efficiencies derived from standardization. Opt in/out programs would substantially increase customer costs or prevent the deployment of smart meters altogether.

- **Historically utilities have had the total discretion in choosing meters for deployment in the field. The deployment of advanced technology meters should remain at the discretion of utilities.**
- **The collection and use of customer energy consumption data by the utility for billing purpose must not be constrained, whether or not a smart meter is involved.**
- **As far as the collection of information on the energy consumption, or the control of, appliances on the customer's side of the meter is concerned, that should be subject to an opt in/opt out selection by the customer.**

- **The constraints on the sharing of energy consumption data with third parties that already exist (per Washington State Law) are adequate to cover any additional information that might be collected and transmitted by smart meters.**

Consumers should be able to share data with utilities or third parties as deemed necessary. Previously it was stated that consumers have a right to access their usage information, but do not own it. Also previously stated the utility should not disseminate detailed consumption data with parties other than the consumer. The consumer may want to provide consumption data to third parties for a myriad of reasons. The most efficient way to satisfy this requirement is for the utility to provide the consumption information to the consumer who is free to pass it along to any third party it desires. It would be beneficial if the consumer was limited to receiving the data in some standard format in order to alleviate the need to export data to an unlimited number of potential data formats.

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

The existing utility commission complaint procedures in each state should continue to be used for smart meter concerns or problems. Both the utilities and the regulatory commissions have the processes in place to process and address customer complaints and concerns. In Washington Customers are made aware of the complaint process via annual disclosure statements inserted into bills, as mandated by state law. Web portal access is a suggested solution for customer self diagnosis prior submission of a complaint.

(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?

Avista currently has strong ties with community action organizations across its service territories. These organizations work with Avista to assist low income customers with the payment of their utility bills. Assistance is also provided to customers, such as the elderly and handicapped, with special needs.

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

Privacy is more of a legal issue than a standards issue. Smart meters should only transmit power consumption data and not personal identification information, addresses, telephone numbers or payment history. Assuming the actual transmittal of power consumption data from smart meters is encrypted, the principal vulnerability in the handling of this information stems from the use of third-party service providers, under contract with the utility, to receive, process and communicate the information back to the customer and the utility.

(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?

Consumers should be free to opt into or out of arrangements with third party providers of "apps," wireless, or hard-wired energy monitoring, auditing, and control applications.

(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?

Research conducted in June 2010 found that there is substantial case law holding that there is no legitimate expectation of privacy with respect to utility records. These cases, however, predated the use of "smart" meters which go beyond the recording of electrical consumption on a month to month basis and may provide time of day usage and the power consumption of individual appliances on the customer's side of the meter.

The following provides the statutory requirements related to utility customer information privacy and how they are implemented in the disclosure statement of Avista's information policy (applicable to Washington and Idaho):

WAC 480-100-153 "Disclosure of private information"

(1) An electric utility may not disclose or sell private consumer information with or to its affiliates, subsidiaries, or any other third party for the purposes of marketing services or product offerings to a customer who does not already subscribe to that service or product, unless the utility has first obtained the customer's written permission to do so.
(2) Private consumer information includes the customer's name, address, telephone number, and any other personally identifying information, as well as information related to the quantity, technical configuration, type, destination, and amount of use of service or products subscribed to by a customer of a regulated utility that is available to the utility solely by virtue of the customer-utility relationship.
(3) This section does not prevent disclosure of the essential terms and conditions of special contracts as provided for in WAC 480-80-143 (Special contracts for gas, electric, and water companies).
(4) This section does not prevent the utility from inserting any marketing information into the customer's billing package.
(5) The utility may collect and release customer information in aggregate form if the aggregated information does not allow any specific customer to be identified.

RCW 19.29A.020 "Disclosures to retail electric customers" requires that the following be provided to customers:

(7) An explanation of the utility's policies governing the confidentiality of proprietary customer information, including the circumstances under which the information may be disclosed and ways in which customers can control access to the information.

This is Avista's current customer information privacy disclosure statement:

It is the policy of Avista Utilities to protect the privacy of our customers and to safeguard any customer information we collect during the course of providing electric and natural gas energy services. Private customer information collected includes customer's name, service address, mailing address, telephone number, a personal identifier (such as, but not limited to, social security number) as well as information related to the type of service, the quantity of electricity or gas consumed and the customer's payment history.

Only authorized and trained Avista employees or authorized representatives have access to or handle customer information. Customer information is stored and processed in secure computer facilities and is accessible by Avista employees or authorized representatives only on a need to know basis.

Avista will not disclose or sell customer information to its affiliates, subsidiaries or third parties for the purposes of marketing services or product offerings to a customer, unless Avista obtains the customer's written permission.

Avista may otherwise provide customer information to government agencies, and to collection agencies (in the event of non-payment of utility bills), but only after verifying the identity and affiliation of the receiving party.

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

Current utility cyber security controls should be incorporated to prevent unauthorized access of consumer information. Personal customer information should not be accessible from smart grid field devices.

(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 Smart Grid can be described as a system of systems. Each utility's version of the Smart Grid may be different due to geography, weather, system configuration, load types, energy sources, and a whole range of other influences. The Department of Energy can play a part, as it already has, in establishing interoperability standards and providing research and development opportunities that are not practical for individual utilities to undertake. Additionally DOE may assist local agencies if requested, to help reach agreement or create solutions across jurisdictional boundaries.

Utility companies must comply with the regulatory desires of local, state, regional, and federal agencies. Local regulation is preferred to insure that regulation is applicable to local needs and does not inflate costs or create operational risks. Layered jurisdictions can delay projects, increase costs, create conflict and ultimately cost consumers in the form of higher utility bills.

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

Federal and state case law has held that government agencies may have unlimited access to energy consumption data maintained by investor-owned utilities through the use of subpoenas and warrants. Municipal utilities and PUD's may be constrained by state constitution privacy provisions which may limit their ability to share customer information with law enforcement.

(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?

Aggregated energy consumption information at the City, Town, County or State level should be in the public domain. Many municipalities tax utilities on the gross receipts from the sale of electricity within the municipality and therefore require such information. Such records must also be shared with state utility commissions and are essential for the utility's ability to demonstrate that it can meet long range regional capacity demands.

Sharing energy consumption information of individual consumers with utility affiliates, subsidiaries and third parties for commercial purpose should be strictly done on an opt-in/opt-out basis.

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

Consumers should not have ownership of, but should have access to, their consumption information in a manner that is economically feasible for the utility to provide. Third party access, if allowed, should be facilitated by the consumer either passing along the information they already have been provided or entering into an agreement to allow access that authorizes release. This information would be provided by consumption interval as measured and subsequently validated.

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

Smart meters may be capable of providing access to consumption information in real or near real-time. If a meter with this capability is available, the consumer may receive from the utility or purchase from the utility, or a third party, an in-home device that allows viewing of consumption information. The viewing device should register with the meter so as to protect consumption data. Customer data should not be stored within the meter or the viewing device.

.

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

It is our understanding that nation-wide, no state regulations currently exist regarding smart grid-related statutes or regulations.

(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?

Avista does not have any plans at this time to revise its existing customer information protection policies.

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

The DOE should have an interest in maintaining consumer privacy as well as data access while evaluating future DOE Smart Grid grant applications.

Respectfully submitted,

Avista Corporation

Marc Schaffner, Director of Business Process Improvement - DO

1411 E Mission Ave

Spokane, WA 99252-0001

509-495-4113