(1) Who owns energy consumption data?

In establishing who owns energy consumption data, it is useful to distinguish between the types of energy consumption data. We separate this data into three types: (A) personally identifiable information, (B) granular consumption data, and (C) aggregate consumption data. Granular data may or may not include personally identifiable information. Aggregate consumption data does not include personally identifiable information.

Personally Identifiable Information (PII)
Personally identifiable information, as it relates to energy consumption data, typically includes a combination of an individual's name and address.

We note that many States have passed privacy laws that define "Personally Identifiable Information" differently. Typically State privacy laws define PII as some combination of: name, social security number, banking information and/or medical information. We are not aware of any energy data collection programs that collect social security numbers, banking information or medical information.

Granular consumption data (GCD)
Granular consumption data provides detailed information about a specific individual's or household's energy consumption. One can infer patterns of behavior of an individual or household from this granular consumption data. GCD might include, for example, the amount of power consumed by a household, stated hour-by-hour or day-by-day. This information, over time, would provide hourly or daily power usage patterns. GCD also might include usage information that correlates with the types of devices in the home, for example, power usage patterns that are associated with the use of a toaster or the charging of an electric vehicle.

GCD does not necessarily include any personally identifiable information. For example, GCD may provide detailed information about when an individual uses his or her toaster, without identifying the name or address of the individual.

Regardless of whether GCD contains or does not contain PII, granular consumption data is data that individuals or members of a household create through their personal efforts and activities.

GCD that does not contain PII should be owned by the individual or household which created the GCD. Similarly, GCD that does contain the name or address data should be owned by the individual or household which created the GCD.

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com

Aggregate data (AD)
Aggregate data is data assembled by the utility from multiple individuals or households; it provides information about patterns of energy consumption on a neighborhood or other regional level. Aggregate data does not include PII and cannot be associated with any individual or household. As a practical matter, this data cannot be owned by an individual because the data does not correlate to any one individual and was not created by any one individual. The data cannot be owned by a group of individuals because the data was not created by any specific group. Also, ownership of the data by a group would require the utility to notify the members of the group and then require the group to organize formally in order to manage the ownership of this data together. All of this is impractical. Aggregate Data is logically the property of the utility.

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

In deciding who should be entitled to privacy protections, it is useful to ask the converse: who might be interested in having access to the information? In addition to the utilities actually providing power, some candidates include:

- Energy-related information providers (e.g., portals)
- Law enforcement agencies
- Commercial enterprises of many sorts
- Criminals
- Insurance companies
- Civil litigants

These groups would seek access to the information because consumption data can reveal activities and information about activities inside the home that have long been understood to be private, such as the time that members of a household wake up and go to sleep, cooking and eating schedules, driving habits, the size of the household, the legality of activities in the home, and even lifestyle and health-related data. Consistent with the general notion of the home as a place in which privacy is expected, individuals household members are entitled to privacy protection for granular information relating to their energy usage. Consequently, we conclude that individuals and households are entitled to privacy protection of GCD.

However, aggregate data does not include individually identifiable information. Consequently, individuals and households do not have a reasonable expectation of privacy in AD and are not entitled to privacy protections relating to AD energy information. Protection of aggregate data from disclosure should be the duty of the utility, based on the utility's operational security programs rather than protection of "privacy".

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com

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

We address this in more detail in response to questions below. In brief, we suggest that privacy practices be based upon the following principles:

- Privacy policies must first define what is and what is not "personally identifiable information" to be protected. This definition may vary based on regional understanding
- Consumers should know what information is being collected and how it is used, and by whom
- The primary purposes for the collection of the data ought to be
    - Empowering consumers to understand and control their energy use
    - Enabling utilities to manage the grid efficiently and economically
- Additional uses of the data (beyond the primary purposes) ought to be permitted only with consumer informed consent
    - Consent can be given either on an opt-in or an opt-out basis, as long as the choice is made knowingly
- If the data is sought by law enforcement agencies or civil litigants, well-established bodies of law for collecting individual information should be observed, e.g., the law concerning warrants for criminal investigations
- Utilities and third parties transmitting and/or storing the data should be required to observe data security standards
    - These standards should be defined nationally, so that utilities operating in more than one state are not required to observe differing security protocols

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

Optional consumer participation in smart meter deployments is not recommended. Smart meters will provide significant economic, environmental and energy security benefits to the United States. Smart meters can also help utilities enhance end-use efficiency, optimize grid operations, balance peak supply and demand, and better integrate renewable power. Installing smart meters only for those who choose to use them and traditional meters for all others would undermine these important policy objectives. Such an approach also would also be technically sub-optimal, logistically impractical, and the resultant costs (e.g., lost economies of scale) would easily outweigh any marginal economic benefits. Therefore, as long as consumer privacy is adequately protected, consumers should not be permitted to opt out of smart meter deployment. (Note: This assertion does *not* require or even imply mandatory consumer participation

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com

in smart meter-enabled initiatives, such as dynamic pricing or peak load control programs.)

Consumers should indeed have control over the granular, personally-identifiable information that is shared with utilities and others. We believe that the choice of consent mechanism, whether opt in or opt out, should be left to the utilities and the marketplace to determine. In either case, end consumers will have final control over how their PII is shared. As long as notice is given in a clear and conspicuous manner, and the method for opting is equally clear, either approach should be permitted.

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

No comment

(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?

Disadvantaged customers - including but not limited to low-income rate payers, those with low literacy, and consumers with limited, if any, broadband access - merit particular consideration. In many cases, these disadvantaged customers stand to benefit from the smart grid, in that many can be expected have high motivation to take control of their energy consumption using smart grid-enabled information and tools to reduce their utility bills. Also, it is generally recognized that customers with relatively flat load profiles subsidize customers with “peak-ier” energy consumption…and low-income customers in many regions often have flatter load curves than average, putting them in a position to benefit from more efficient allocation of costs than can be achieved through smart grid-enabled dynamic pricing.

On the other hand, disadvantaged customers can prove challenging to engage, due to language, cultural, geographic, and other barriers. Experience to date has shown that customer engagement greatly enhances the effectiveness of smart grid technologies. This suggests that resources for customer engagement should be tailored to ensure outreach to disadvantaged customers by using targeted approaches and specialized methods (e.g., grassroots and community organizations, multi-lingual communications across a wide range of media, etc.).

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

Attempting to define privacy standards that will be suitable worldwide would be unwise. Privacy is a cultural notion, and cultures differ in the aspects of life that they consider to

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com

be private, and the manner in which they seek to safeguard their privacy. For example, In Italy, executives of search engine company Google were recently convicted of a crime of violating the privacy of a child with autism who was shown being bullied in a video that a user posted on Google's site. In the U.S. legal regime, online service providers are generally not held accountable when one of their users posts material that invades someone else's privacy. While there is no general right of privacy in the UK, France has privacy laws that restrict disclosure of information gleaned by searching through garbage. Canada has at least 8 privacy laws applicable to the private sector, and others applicable to the government.

Even within the United States, no single regime or law addresses the issue of privacy. Instead, we have privacy provisions in constitutions, privacy laws established in civil and criminal court decisions, and hundreds of discrete statues at the state and federal level.

Similarly, a fair number of "privacy principles" have been articulated, such as the U.S. Department of Health Education and Welfare's "Fair Information Practices" (1973)i and the Department of Homeland Security's Fair Information Practices (2008)ii.

We suggest that the following principles should apply:

- Privacy policies must first define what is and what is not "personally identifiable information" to be protected. This definition may vary based on regional understanding
- Consumers should know what information is being collected and how it is used, and by whom
- The primary purposes for the collection of the data ought to be
    - Empowering consumers to understand and control their energy use
    - Enabling utilities to manage the grid efficiently and economically
- Additional uses of the data (beyond the primary purposes) ought to be permitted only with consumer informed consent
    - Consent can be given either on an opt-in or an opt-out basis, as long as the choice is made knowingly
- If the data is sought by law enforcement agencies or civil litigants, well-established bodies of law for collecting individual information should be observed, e.g., the law concerning warrants for criminal investigations
- Utilities and third parties transmitting and/or storing the data should be required to observe data security standards
    - These standards should be defined nationally, so that utilities operating in more than one state are not required to observe differing security protocols

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com

(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?

As noted in responses to question 7, no single data privacy standard fits all needs. "Reasonable expectations" as to what information ought to be private vary from community to community. On the other hand, having varying data requirements in different jurisdictions will thwart rather than promote innovation and experimentation.

The solution is to require a threshold of procedural safeguards, including meaningful disclosure and clear and simple opportunities to give or withhold consent, so that consumers empowered to make meaningful choices about the use of their data. As long as these requisites are in place – information and choice -- privacy interests are protected while leaving room for innovation and creativity.

(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 potential benefits and detriments of both privacy and access?

Meaningful choice can only be made when the consumer is informed. Today, most written privacy policies describe the types of information that might be collected and disclosed, and to whom, often with vague statements of purpose such as "to provide marketing activities and services." What is generally lacking is an explanation of the benefit to the consumer of the disclosure and, conversely, the disadvantage to the consumer if he or she were to opt out. We would encourage industry to bolster their privacy statements in this respect.

Even if the consumer has sufficient information, recent efforts by Facebook illustrate the difficulty in striking the right balance between too little control over privacy choices and too much. When the company adopted a multi-tiered, highly granular system of privacy controls, it was widely criticized for making the settings to complex.

With regard to the potential tradeoffs between cost and access (e.g., "access" implies cost and compromising privacy might be a cost mitigation), we believe that there needs to be a standard for making basic information available directly to consumers that does not require any release of PII to third parties. For example, utilities can make some defined set of information available directly to all consumers from their respective smart meters (e.g., via HAN or web portals) without risking privacy compromise from third party participation. The cost for making that level information accessible would be

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com

modest and should be considered reasonable and prudent, and thus recoverable by utilities across the broad rate base.

Additional/premium information access services may cost more, and the possible approaches are myriad. Consumers might be willing to pay for these services on their own, they may obtain them from third-parties in exchange for PII release, etc. We do not know how yet these models will evolve, but we believe that they should not be precluded.

In summary, consumers should be able to gain basic access to their own data without privacy risks from third party involvement, but third party participation should not be excluded from providing more advanced services.

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

- Smart grid communications systems should be designed with at least a 20-year threat model in mind, since these devices have limited, if any, physical protection in the field and are unlikely to be cost-effectively retrofitted in the field once deployed.
- Robust cryptography based on publicly-development and field-hardened standards (e.g., NSA-approved AES encryption) should be required
- Retail attacks (e.g., compromise of individual endpoints) must be categorically prevented from escalating into wholesale attacks (e.g., compromise of entire categories of devices or the network itself), through unique authentication systems and role-based authorization procedures.
- Over-the-air firmware upgrades must employ proven encryption, authentication, and role-based authorization techniques.
- Critical functions, such as remote disconnects, should be additionally hardened with advanced technological and physical security measures.

(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?

No comment

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

Laws regulating government access to private data are well established. In the criminal arena, for example, the Fourth Amendment establishes a baseline protection against search, and decades of court decisions have defined the circumstances under which a

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com

warrant is or is not required. Statutes such as the U.S. Patriot Act establish other guidelines for the collection of data by the government. Similarly, many states have statutes with safeguards regulating the state and local government access to private data. We do not believe that a new, separate mechanism is required simply because the data in question is energy consumption data. Instead, established procedural and constitutional safeguards should be applied.

(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 not should not be given broad, unfettered access to data, even if the data is aggregated or anonymous. There is simply too much risk in release of this data outside of the controls of customer-specific release.

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

A basic set of information that includes interval consumption and aggregate data should be made available to consumers (and/or their designated third-party) at no cost. Consumers should also be provided a means to accessing "real time" data directly from the meter, either via recognized HAN technology standards or, at additional expense, via a physical interface for pulse-outputs from the meter (e.g., KYZ or RS485 outputs). For the purposes of this discussion, the only third-party release should be where the consumer has designated a third-party to act as their agent.

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

There is considerable enthusiasm presently for giving consumers access to real-time or near real-time information, reflecting the variations in the cost of generating and delivering electricity at different times of day. However, we would submit to the DOE that giving consumers access to a time-differentiated *price* signal is the most useful information, since it is at periods of peak prices that consumers will most benefit from curtailing consumption. On a real-time or near real-time basis, consumers are arguably more interested in knowing *when* to avoid peak prices, versus their desire to know the *amount* of kilowatt-hours they have consumed up at any instant.

Actual consumption data from the meter will not be revenue-grade until it has been processed by utility backoffice systems. There is no reason that on-meter consumption data should not be accessible, so long as it is clear to consumers that this is only estimated.

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com

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

No comment.

(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?

No comment.

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

No comment.

---

[i] 1. There must be no personal data record-keeping whose very existence is secret
2. There must be a way for a person to find out what information about the person is in a record and how it is used
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent
4. There must be a way for a person to correct or amend a record of identifiable information about the person
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precaution to prevent misuses of the data

[ii] Transparency
Individual Participation
Purpose Specification
Data Minimization
Use Limitation
Data Quality and Integrity
Security
Accountability and Auditing

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com