Public Comment on the Consumer Interface with the Smart Grid

February 19, 2010

We appreciate the opportunity to provide OSTP with information about the interface between consumers and the Smart Grid.[1] Consumers have a significant interest in the privacy of Smart Grid-related data. They should also be able to benefit from competition and innovation among device and service providers. Finally, all members of society share an interest in ensuring that the power grid is reliable and resilient to failures—whether caused by accident or malicious activity—as digital information technology become more heavily integrated into the grid.

PROTECTING DATA PRIVACY WILL PROMOTE OTHER SMART GRID POLICY GOALS

In this brief comment, we point out that Smart Grid technology can bring all of these interests into alignment, but doing so requires closely examining how policy decisions—from the adoption of federal technical standards to state utility commissions' review of Smart Grid infrastructure investments—will affect all of these interests. At the federal level, NIST-led efforts have yielded thorough, thoughtful documents that make significant progress in addressing interoperability and cybersecurity. Though these documents recognize the importance of Smart Grid data privacy, they do not fully develop privacy requirements.

OSTP should encourage NIST and other federal agencies to give full consideration to Smart Grid privacy risks without delay. Smart Grid data has the potential to reveal a great deal of information about activities within a household. A recent analysis based on experimental energy usage correctly inferred more than 90% of the time whether the residence under study was occupied and whether occupants were awake or asleep.[2] Such detailed data could help improve service and influence peak energy demand. But it also has a potentially wide array of secondary uses, such as providing marketers with information. This data also has obvious value to burglars, identity thieves, and other malicious actors. We do not present a full analysis of the Constitutional and statutory protections that may apply to this data. Instead, we note that individuals' expectations of privacy in Smart Grid data are likely to attach to the data, irrespective of whether it is routed through a smart meter or through a third-party device.

Smart meters and other technologies are most likely to provide robust privacy protections if they are incorporated by design. Neglecting privacy in the near term could expose consumers to unnecessary privacy risks and require costly retrofitting or replacement of infrastructure down the road. If consumers do not trust the technologies and organizations that make the Smart Grid run to protect their privacy, they will hesitate to adopt new technologies and participate in demand response and other modernization programs. This, in turn, will make it more difficult to

---

[1] *See* Office of Science and Technology Policy, Notice and Request for Public Comment on the Consumer Interface with the Smart Grid, 75 Fed. Reg. 6414 (Feb. 9, 2010), http://edocket.access.gpo.gov/2010/2010-2813.htm.

[2] *See* Mikhail A. Lisovich, Deirdre K. Mulligan, and Stephen B. Wicker, *Inferring Personal Information from Demand Response Systems*, IEEE SECURITY & PRIVACY, Jan./Feb. 2010, 11-20.

reduce peak energy demands, integrate renewable energy sources, and meet the other national goals established by Congress. We discuss how to relate the goals of privacy, cybersecurity, and innovation in the context of several of the questions OSTP posed in its Request.

RESPONSES TO SPECIFIC RFI QUESTIONS

RFI Question 1. Should the smart meter serve as the primary gateway for residential energy usage data, price data, and demand response signals? What are the most important factors in making this assessment, and how might those factors change over time?

Any analysis of the privacy, security, and innovation issues raised by making the smart meter into the home's primary energy data gateway must begin with a recognition that states that have led the way in Smart Grid deployment have already endorsed this architecture. The California Public Utilities Commission (CPUC), for example, has approved plans by the three major investor-owned utilities in the states to deploy smart meters that have an embedded controller for devices within the home,[3] implying that the meter will serve as a gateway usage data, price data, and demand response signals. Other regulations lay the groundwork for utilities to collect home energy usage data with increasing frequency as the state's smart meter initiative matures. Similarly, in a rule adopted by the Texas Public Utilities Commission requires advanced meters that provide a "capability to communicate with devices inside the premises, . . . through a home area network (HAN), based on open standards and protocols that comply with nationally recognized non-proprietary standards such as ZigBee, Home-Plug, or the equivalent."[4]

The privacy risks in this architecture are still unclear; they depend in large part on future decisions by consumers, utilities, and state regulators. On one hand, utilities are the most likely recipients of this data, making it relatively easy for consumers and regulators to monitor their privacy practices. On the other hand, if utilities are granted exclusive access to this data, they will not be subject to other energy management services that may compete on privacy and other dimensions. Much to its credit, the CPUC has modified rulemaking to extend to data privacy,[5] but it will necessarily develop these rules after millions of smart meters containing data gateways are already in place. Other states will presumably follow California's lead, but state-by-state decisions could impose duplicative costs and create inconsistent rules. Moreover, though public utilities commissions have broad expertise in consumer protection issues, it is less clear that they possess specific, deep expertise in data privacy.

Two further points about making smart meters into energy data gateways bear on both privacy and innovation. First, utilities and device manufacturers will use this data to control

---

[3] *See* Home Area Network (HAN) Overview, Pacific Gas & Electric Company, Jan. 2009, www.edisonfoundation.net/iee/issueBriefs/PG&E_HAN_January_2009.pdf.

[4] Tex. Admin. Code, tit. 16, § 25.130(g)(1)(J).

[5] Cal. Pub. Utils. Comm'n, *Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's Own Motion to Actively Guide Policy in California's Development of a Smart Grid System* 78 (Decision 09-12-046, Dec. 17, 2009), http://docs.cpuc.ca.gov/word_pdf/FINAL_DECISION/111856.pdf (ordering further proceeding to consider usage and price data access rules).

device behavior. This creates a need to designate which devices will respond to demand response signals, and how. In use cases considered within prominent standards and in state Smart Grid proceedings, the utility is often responsible for registering consumers' devices.[6] This not only constrains the choices available to device manufacturers but also creates the possibility that utilities (and, perhaps, third parties they authorize) will have access to device-specific usage data. This would further exacerbate the privacy risks entailed in collecting highly temporally resolved, household-specific usage data. Second, the choice between on-meter and off-meter gateways need not be binary. Even if consumers are served by utilities that deploy smart meters with embedded gateways, they should be able to choose to use third-party gateways.[7] A full analysis of the privacy risks of both architectures would help inform these choices.

Federal agencies such as NIST could marshal the efforts of all stakeholders to analyze the privacy risks in this architecture. A comment filed by the Center for Democracy & Technology on NIST's draft Smart Grid cybersecurity requirements provides a start by laying out how widely Fair Information Practice Principles (FIPPs) apply to Smart Grid data. As that comment notes, however, additional work, such as developing privacy use cases, is necessary to fully understand the privacy risks of smart meters with an embedded gateway. This analysis would provide valuable guidance to technology firms and state policymakers.

RFI Question 2. Should a data gateway other than the smart meter be used for all or a subset of the data described in question 1?

Considering an alternative architecture—routing Smart Grid through a home Internet connection, for example—gives a sense of the relative risks to privacy, innovation, and cybersecurity. An off-meter gateway could help protect consumers' privacy by limiting the amount of information that is sent beyond the boundaries of the home. For instance, a gateway that is separate from the meter could receive incoming price and demand response signals, send them to an in-home energy management system (EMS), and, in conjunction with the EMS, manage devices solely through in-home communications. This architecture would obviate any need to register appliances and other devices with a utility, further limiting the disclosure of information from inside the home. The smart meter, of course, would still be able to measure and report energy consumption to the utility.

Still, fully understanding the privacy risks of such this architecture requires a more detailed analysis of specific technologies and their uses. Again, relevant policy considerations include (1) whether consumers have ongoing choices about how much data to disclose about

---

[6] *See, e.g.*, Southern California Edison (SCE), SmartConnect Use Case: C6 – Customer Uses and Energy Management System (EMS) or In-Home Display (IHD), Jan. 5, 2009, http://www.sce.com/NR/rdonlyres/EC46A2AC-9D43-4674-90A7-CBE47F362CDE/0/C5_Use_Case_090105.pdf. NIST considered this and other SCE use cases in its Interoperability Framework and its draft Cyber Security Strategy.

[7] This statement also relates to OSTP's request for comments on allowing third-party access to data if the primary gateway is on the smart meter and alternative architectures to support innovation (Questions 3 and 6, respectively). The privacy risks in those cases largely track our analyses under Questions 1 and 2, above.

their energy use; (2) what type(s) of entities that receive and process this data; and (3) which regulators (if any) have jurisdiction over those entities. It is possible that neither a data gateway outside the smart meter nor the entities that provide services based on data flowing through that gateway will be subject to state utility commission authorities. Though this could give rise to competition among device and service providers, it also raises the question of how to encourage those firms to build privacy into their products.

Comparing the cybersecurity risks of these two architectures is also difficult to do in the abstract. Maintaining the availability of electricity service is a fundamental requirement of the Smart Grid. The integrity of price, usage, and demand response data is crucial for consumers and utilities. The price and demand response signals that consumers receive must be correct. Likewise, the usage data that utilities receive must be free from corruption, whether introduced by malicious attacks or accidental errors, in order to manage load and to bill customers correctly. However, certain security benefits of separating the smart meter from demand response and home area network traffic are evident: this architecture would isolate the meter from devices in the home. It would also simplify the functional requirements of the smart meter, which should make the task of securing this critical Smart Grid element easier.[8]

Evaluating the security of different architectures and implementations is an enormously complex task. But this complexity lends itself to a simple point: statements about the Smart Grid security are most meaningful when they pertain to a specific system, are explained through a clearly stated threat model, and are supported by an analysis that is open to scrutiny.

RFI Question 4. Who owns the home energy usage data? Should individual consumers and their authorized third-party service providers have the right to access energy usage data directly from the meter?

To the extent that "ownership" of data implies that one person or entity has an exclusive (but transferable) right to use data, it is too simplistic a notion to apply in the context of home energy usage data.[9] Instead, it is more helpful to refer to the rights and obligations of the relevant actors, including consumers, utilities, and third parties. As stated above, consumers have a strong interest in controlling how data relating to their energy use is collected, used, and disclosed. These expectations should be backed up by technology and further analysis of privacy risks. Moreover, privacy expectations are likely persist, irrespective of whether consumers consent to allow third parties to handle their data in any manner the agreement discloses. Accordingly, thinking in terms of rights and obligations will likely lead to more robust data privacy protections than focusing narrowly on the notion of data "ownership."

[8] A maxim of computer security holds that "complexity is the enemy of security."
[9] *See* Pamela Samuelson, *Privacy as Intellectual Property?* 52 STAN. L. REV. 1125 (2000), draft version available at http://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf (critiquing a property-based view of personal data on descriptive and normative grounds).

CONCLUSION

OSTP should promote a full analysis of Smart Grid privacy risks, following the model of NIST's cybersecurity analysis. This analysis would help firms design privacy protections into their technologies. It would also provide consumers and state regulators with valuable guidance on the privacy dimensions of the Smart Grid as they adopt Smart Grid technologies.

Respectfully submitted,

Aaron J. Burstein[*]
Longhao Wang[*]
University of California, Berkeley
School of Information
Berkeley, CA 94720

Ari Schwartz
Vice President and Chief Operating Officer
Center for Democracy & Technology
1634 I Street NW, Suite 1100
Washington, DC 20006

[*] Institutional affiliation is provided only for purposes of identification. These comments do not purport to represent the official views of the University of California. The authors may be contacted by email: aaron.burstein@gmail.com and longhao@berkeley.edu, respectively.