

# TOWN OF FAIRFAX STAFF REPORT

**TO:** Mayor and Town Council

**FROM:** Michael Rock, Town Manager



**DATE:** August 4, 2010

**SUBJECT:** Discussion/Consideration of an urgency measure establishing a temporary moratorium on the installation of Smart Meters and related equipment within the Town of Fairfax or in, along, across, upon, under and over the public streets and places within the Town of Fairfax, and declaring the urgency thereof

## RECOMMENDATION

The Town Council considers adopting an emergency ordinance establishing a moratorium on the installation of smart meters and related equipment within the Town of Fairfax or in, along, across, upon, under and over the public streets and places within the Town of Fairfax, and declaring the urgency thereof.

## DISCUSSION

At the July 7, 2010 Town Council meeting the Town Council took several actions related to the smart meters including directing staff to draft an ordinance that would establish a moratorium on the installation of smart meters in the Town of Fairfax. Attached to this staff report is the proposed ordinance which can be adopted this evening as an urgency ordinance with a 4/5 vote.

Also attached to this staff report is a letter written by Vice Mayor Bragman to the CPUC requesting the CPUC suspend deployment of the smart meter program. The final attachment is a memo written by the UC Berkeley School of Information regarding smart meters and privacy issues.

## FISCAL IMPACTS

Minor staff time costs to prepare the ordinance.

## ATTACHMENTS

1. Ordinance establishing a moratorium on the installation of smart meters in the Town of Fairfax
2. Vice Mayor Bragman letter to the CPUC
3. Memo written by the UC Berkeley School of Information regarding smart meters and privacy issues

ORDINANCE NO. 752

AN ORDINANCE OF THE TOWN COUNCIL OF THE TOWN OF FAIRFAX ADOPTED AS AN URGENCY MEASURE ESTABLISHING A TEMPORARY MORATORIUM ON THE INSTALLATION OF SMARTMETERS AND RELATED EQUIPMENT WITHIN THE TOWN OF FAIRFAX OR IN, ALONG, ACROSS, UPON, UNDER AND OVER THE PUBLIC STREETS AND PLACES WITHIN THE TOWN OF FAIRFAX, AND DECLARING THE URGENCY THEREOF

The Town Council of the Town of Fairfax, California does ordain as follows:

Section I. Findings:

- A. The Town of Fairfax (the "Town"), through its police powers granted by Article XI of the California Constitution, retains broad discretion to legislate for public purposes and for the general welfare, including but not limited to matters of public health, safety and consumer protection.
- B. In addition, the Town retains authority under Article XII, Section 8 of the Constitution to grant franchises for public utilities, and pursuant to California Public Utilities Code section 6203, "may in such a franchise impose such other and additional terms and conditions..., whether governmental or contractual in character, as in the judgment of the legislative body are to the public interest."
- C. Further, Public Utilities Code section 2902 reserves the Town's right to supervise and regulate public utilities in matters affecting the health, convenience and safety of the general public, "such as the use and repair of public streets by any public utility, the location of the poles, wires, mains, or conduits of any public utility, on, under, or above any public streets, and the speed of common carriers operating within the limits of the municipal corporation."
- D. Pacific Gas & Electric Company ("PG&E") is now installing SmartMeters in Central and Northern California and will be installing these meters in Fairfax in the very near future. PG&E has already installed antennae to support the SmartMeter system at four sites within the public rights of way in the Town without obtaining permits from the Town as required by Section 19.04 of the Town Code. Further, PG&E did not comply with Section XIV of General Order 131-D of the California Public Utilities Commission (the "CPUC"), which requires a utility to consult with the local jurisdiction on land use matter prior to locating its facilities.
- E. Concerns about the impact and accuracy of SmartMeters have been raised nationwide, leading the Maryland Public Service Commission to deny permission on June 21, 2010 for the deployment of SmartMeters in that state. The CPUC currently has pending before it a petition from the City and County of San Francisco, the Town of Fairfax and other municipalities, seeking to delay the implementation of SmartMeters until the questions about their accuracy can be evaluated.

- F. Indeed, major problems and deficiencies with SmartMeters in California have been brought to the attention of the Fairfax Town Council, including PG&E's confirmation that SmartMeters have provided incorrect readings costing ratepayers untold thousands of dollars in overcharges and PG&E's records outlined "risks" and "issues" including an ongoing inability to recover real-time data because of faulty hardware originating with PG&E vendors.
- G. The ebb and flow of gas and electricity into homes discloses detailed information about private details of daily life. Energy usage data, measured moment by moment, allows the reconstruction of a household's activities: when people wake up, when they come home, when they go on vacation, and even when they take a hot bath. SmartMeters represent a new form of technology that relays detailed hitherto confidential information reflecting the times and amounts of the use of electrical power without adequately protecting that data from being accessed by unauthorized persons or entities and as such pose an unreasonable intrusion of utility customers' privacy rights and security interests. Indeed, the fact that the CPUC has not established safeguards for privacy in its regulatory approvals may violate the principles set forth by the U.S. Supreme Court in *Kyllo v. United States* (2001), 533 U.S. 27.
- H. Significant health questions have been raised concerning the increased electromagnetic frequency radiation (EMF) emitted by the wireless technology in SmartMeters, which will be in every house, apartment and business, thereby adding additional man-made EMF to our environment around the clock to the already existing EMF from utility poles, individual meters and telephone poles.
- I. FCC safety standards exist for chronic long-term exposure to EMF or from multiple sources, and reported adverse health effects from electromagnetic pollution include sleep disorders, irritability, short term memory loss, headaches, anxiety, nausea, DNA breaks, abnormal cell growth, cancer, premature aging, etc.. Because of untested technology, international scientists, environmental agencies, advocacy groups and doctors are calling for the use of caution in wireless technologies.
- J. Because the potential risks to the health, safety and welfare of Fairfax residents are so great, the Fairfax Town Council wishes to adopt a six month moratorium on the installation of SmartMeters and related equipment within the Fairfax Town Limits. The six-month period will allow the CPUC petition process referenced in Recital E above to be completed and for additional information to be collected and analyzed regarding potential problems with SmartMeters.
- K. There is a current and immediate threat to public health, safety and welfare because, without this urgency ordinance, SmartMeters or supporting equipment will be installed or constructed or modified in the Town without PG&E's complying with the CPUC process for consultation with the local jurisdiction, the Town's Code requirements, and subjecting residents of Fairfax to the privacy, security, health, accuracy and consumer fraud risks of the unproven SmartMeter technology.

L. The Town Council hereby finds that it can be seen with certainty that there is no possibility that the adoption and implementation of this Ordinance may have a significant effect on the environment. This Ordinance does not authorize construction or installation of any facilities and, in fact, imposes greater restrictions on such construction and installation in order to protect the public health, safety and general welfare. This Ordinance is therefore exempt from the environmental review requirements of the California Environmental Quality Act (CEQA) pursuant to Section 15061(b)(3) of Title 14 of the California Code of Regulations.

## Section II. Moratorium

1. No SmartMeter may be installed in or on any home, apartment, condominium or business in Fairfax, and no equipment related to SmartMeters may be installed in, on, under, or above any public street or public right of way in the Town for six months from the date of this Ordinance, at which time the Fairfax Town Council, shall consider whether to extend or terminate this prohibition in light of the then-current data on SmartMeter privacy, safety, accuracy and health effects.

2. Violations of this Moratorium may be charged as infractions or misdemeanors as set forth in Chapter 1.08.010 of the Town Code or as administrative citations as set forth in Chapter 1.10 of the Town Code, in the discretion of the Town. In addition, violations shall be deemed public nuisances, with enforcement by injunction or any other remedy authorized by law.

3. The Fairfax Town Manager is hereby authorized to direct all Town Departments, including the Town Attorney, to facilitate compliance with the purpose and intent of this Ordinance using the enforcement powers described in the preceding paragraph.

## Section III. Effectiveness

This Ordinance, being adopted as an urgency measure for the immediate protection of the public safety, health, and general welfare and containing a declaration of the facts constituting the urgency, upon passage by a minimum four-fifths (4/5) vote of the Town Council, shall take effect immediately upon its adoption and shall continue in effect until modified or rescinded.

## Section IV. Severability

If any provision of this Ordinance or the application thereof to any person or circumstances is held invalid, such invalidity shall not affect any other provision or application, and to this end the provisions of this chapter are severable.

## Section V. Publication

Copies of the foregoing ordinance shall, within fifteen days after its passage and adoption, be posted in three public places in the Town of Fairfax, to wit: 1. Bulletin Board, Town Hall Offices; 2. Bulletin Board, Fairfax Post Office; 3. Bulletin Board, Fairfax Women's Club building; which places are designated for that purpose.

The foregoing ordinance was duly adopted on the 4th day of August, 2010, by the following vote,  
to wit:

AYES:

NOES:

ABSENT:

\_\_\_\_\_  
LEW TREMAINE, MAYOR

Attest:

\_\_\_\_\_  
Town Clerk

July 28, 2010

California Public Utilities Commission  
505 Van Ness Avenue  
San Francisco, CA 94102

BY FACSIMILE AND U.S. MAIL: (415) 703-1758

Re: Smart Meter Deployment in the Town of Fairfax

Dear Commissioners:

I am writing to convey my observations about Pacific Gas and Electric Company's deployment of its Smart Meter program in the Town of Fairfax.

The Fairfax Town Council has received numerous written and live comments from local residents who are extremely apprehensive about the ongoing installation of these devices in our Town. Their concerns break down into five broad categories:

1. Health concerns: There is a large percentage of individuals who chose to live in Fairfax because of its pristine environment and its local government's rigorous attempts to adhere to the precautionary principal. The fact that the smart meter program will create a pervasive electromagnetic field (EMF) in our community is of great concern to many residents. Electromagnetic sensitivity has been recognized as a protected condition under the Americans with Disabilities Act and recent peer reviewed literature has suggested potential health risks to chronic exposure. Because the Smart Meter network is a mesh network, its impossible to predict individual levels of exposure. Numerous residents have posted their property with signs demanding that their meters be left in place.

2. Security Risks: The security issues inherent in the Smart Meter program were analyzed in depth by the Maryland Public Service Commission's decision denying a very similar AMI program in Baltimore. At pages 35-40, the Commission stated:

"Cyber-security in the context of the "smart grid" refers to the security of the information passing over the communications of the "smart grid" as well as security of the controls over system components. AMI is an enormous complex of inter-connected networks designed to administer dynamic pricing and manage grid function. Such an extensive network is vulnerable to security risks in many different ways, including physical tampering, intercepting or blocking the wireless signals that connect the smart meters to data collection points, or obtaining customer password

information used on the web portal. Unauthorized access to smart meters could allow a hacker to artificially increase energy bills or shut off power entirely.”

3. Privacy Concerns: There is a growing consensus that the smart meter program does not have adequate privacy controls. The program will generate an unprecedented database of confidential information subject to intrusion and commercial misuse. PG&E has admitted that it currently does not have the capacity to manage the data and the State of California does not have comprehensive Fair Information Practices that provide legal and regulatory guidelines sufficient to safeguard consumer privacy. Further, I believe that the degree of intrusion raises privacy issues of Constitutional dimension under the Supreme Court’s decision in *Kyllo v. U.S.* 533 U.S. 27 (2001) . The enclosed Memorandum from the University of California School of Information summarizes the numerous unresolved privacy issues involved in this program.

4. Accuracy: As the Commission is well aware, there have been hundreds of reports of unexplained billing spikes that have not been resolved. Senator Florez held hearings about those complaints and the Structure Group’s analysis of the accuracy of the Smart Meter system is not complete. Our residents question why these devices are being deployed before the Commission has data that confirms their reliability.

5. Conflicts of Law and Authority: Smart Meter antennae have been deployed in Fairfax’s public rights of way without the consultation of Town Staff. Fairfax’s Wireless Telecommunications Ordinances have long required that any party seeking the installation of wireless antennae obtain a use permit from the Fairfax Planning Commission. (Fairfax Municipal Code Chapter 19.04) I believe that the Town of Fairfax has authority to enforce compliance with its ordinances under Public Utilities Code sections 6203 and 2902.

Given the foregoing, I am respectfully requesting that the Commission suspend deployment of the Smart Meter program until its profound socio-economic, scientific and legal implications are more thoroughly understood and reconciled. Thank you for your time and attention.

Sincerely yours,

LARRY BRAGMAN  
Fairfax Town Council

March 7, 2010

Dr. George W. Arnold, National Coordinator for Smart Grid Interoperability,  
National Institute of Standards and Technology (NIST)  
Office of Science and Technology Policy (OSTP), Executive Office of the President

**Re: Policy Questions on Data Ownership and Access in the Smart Grid**

Dear Dr. Arnold and OSTP Staff:

We thank OSTP and NIST for their interest in the public's views on the consumer interface to the Smart Grid. The transition to the Smart Grid promises great benefits for consumers, including lowered energy costs, increased usage of environmentally friendly power sources, and enhanced security against attack and outage. We are pleased to offer our thoughts on the consumer interface to the Smart Grid, and particularly our thoughts on related consumer privacy issues.

From the perspective of consumers, and particularly from the perspective of consumer privacy, we stand at a critical juncture in the development of Smart Grid. First, the emergence of increasingly sophisticated metering technologies is enabling the unprecedented collection of energy consumption data, removing a "latent structural limitation" that previously protected the revelation of intimate details about household activities.<sup>1</sup> Whereas historically a consumer's consumption data may have been collected once a month or less frequently from a traditional meter fixed to the side of a house, in the Smart Grid, sophisticated new systems will collect and record 750 to 3,000 (or more) data points a month, revealing variations in consumption that can reflect specific household activities such as sleep, work, and travel habits.<sup>2</sup>

Second, the transition to a highly-interconnected and less-bordered electrical infrastructure is inviting participation by new entities, such as third-party service providers offering new web-based portals for managing energy use. As a result, entities other than the utilities will be receiving consumer energy consumption data and using it in new ways, presenting the need for privacy analysis extending beyond the more straightforward consumer-to-utility relationship. Third, the rapid pace of Smart Grid deployment, and the speed at which new Smart Grid technologies are moving out of the pilot project stage to large-scale implementation, are making the consideration of the consumer privacy issues presented by these technologies more urgent. Finally, against this landscape of rapid development, legal protections for home energy usage data are fragmented and unclear. As NIST noted in its First Draft

---

<sup>1</sup> See Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1618 (2007), <http://ssrn.com/abstract=1004675> (noting how "the widespread diffusion of an emerging technology effectively causes a rights-shift with respect to privacy interests protected by latent structural constraints").

<sup>2</sup> Jack I. Lerner & Deirdre K. Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3, 3.

NISTIR 7628, there remains a “lack of consistent and comprehensive privacy policies, standards, and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use,” creating “a privacy risk that needs to be addressed.”<sup>3</sup>

Therefore, there is an urgent need for robust data usage guidelines, based on the full set of Fair Information Practice principles, that can be reflected in business practices, as well as technical standards and requirements, as Smart Grid deployment continues and develops. The time to address consumer privacy concerns is now, while we have the opportunity to thoughtfully build protections into technologies and business practices to better effect, and at a lower cost, than attempting to “bolt on” privacy protections later.

### **OSTP Question 1: Who owns the home energy usage data?**

#### **A. Consumers Should Both Own and Control Home Energy Usage Data.**

Home energy usage data is generated by, and is a reflection of, consumers’ activities within their homes, posing new and substantial risks to individual privacy. This data also has an important role to play in supporting innovations that will help achieve broader energy policy goals in a de-centralized and competitive environment. Accordingly, if anyone “owns” home energy usage data, it should be the utility customers. Assigning data ownership to utilities would turn them into information gatekeepers and could impede realization of both privacy and innovation policy goals. For these reasons, if property rights are the framework being used, consumers should be considered the owners of their home energy use data, and utilities or other holders of energy use data should be considered trustees or custodians of the data, who must handle it with respect for the privacy and other interests of the consumer.

Simply determining that customers “own” this data, however, does not resolve the privacy issues or provide a workable set of rules or principles to govern its use. At its worst, ownership can leave consumers with the limited ability to choose between alienating their data or not. What consumers need is ongoing rights in their data—regardless of where it is stored and who it is held by—complimented by assurances that those to whom they entrust it are bound by clear rules that bind them to abide by consumers decisions. Such a framework respects the ongoing implications such data has for the consumer’s privacy and safety. Rights and responsibilities must be established with regard to the data, and those rights and responsibilities should be established with regard to underlying values of privacy, security, efficiency, interoperability, consumer choice, competition and innovation.

Such a comprehensive policy framework exists in the widely-recognized Fair Information Practice Principles (“FIPs”). The FIPs framework will ensure that all Smart Grid stakeholders have consistent rights and responsibilities in connection with home energy usage data. The issues of use, retention, sharing, access, security, and other components of FIPs need to be answered regardless of who “owns” the data.

---

<sup>3</sup> NIST, *Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements*, <http://www.nist.gov/smartgrid/>.

We urge OSTP to recognize and promote the use of the Fair Information Practice principles, as outlined in detail below, to manage the collection and use of home energy usage data.

**B. Privacy Interests in Home Energy Usage Data Require the Robust, Comprehensive Application of Fair Information Practice Principles.**

Consumers have strong privacy interests in home energy usage data because it pertains to activities within a physical and associative domain—the home—that United States law and culture recognize as a locus of individual autonomy and family intimacy. Smart Grid deployment will introduce an entirely new avenue for exposing information about household activities. It would be anomalous to fail to protect this data against unforeseen uses by entities that receive it directly from consumers (e.g., utilities, application or service providers) as well as against disclosures to law enforcement agencies or other third parties.

The potential for home energy usage data to reveal a great deal about in-home activities is clear. For example, a recent analysis demonstrated that home energy usage data collected at a resolution that is well within current smart meter capabilities permits extremely accurate inferences about whether a home is occupied and whether its occupants are asleep or awake.<sup>4</sup> Traces of energy usage over time may also contain signatures of certain appliances—refrigerators and toasters, for example—that are so clear they require little or no analysis to detect.<sup>5</sup> Moreover, technical standards for meters and other smart devices would add information about specific devices to this mix. The ZigBee Smart Energy Profile Specification, for example, specifies a data field that declares the type of device that is in use (e.g., interior lighting, water heater, etc.). California utilities are deploying smart meters that are capable of taking usage readings every five seconds.<sup>6</sup>

This type of information about home appliance use will reflect intimate details of people's lives and their habits and preferences inside their homes. As Justice Scalia recognized in *Kyllo v. United States*, “at what hour each night the lady of the house takes her daily sauna and bath” is “a detail that many would consider ‘intimate.’”<sup>7</sup> Some of the activities that might be revealed through the Smart Grid include personal sleep and work habits, cooking and eating schedules, the presence of certain medical equipment and other specialized devices, and

---

<sup>4</sup> 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.

<sup>5</sup> See Elias Leake Quinn, *Smart Metering & Privacy: Existing Law and Competing Policies* v, 3 (Spring 2009) (providing examples).

<sup>6</sup> Calif. Energy Comm'n, *Proposed Load Management Standards (Draft Committee Report)* 25, CEC-400-2008-027-CT, Nov. 2008, at <http://www.energy.ca.gov/2008publications/CEC-400-2008-027/CEC-400-2008-027-CTD.PDF> (“The meters [being deployed by California’s three major investor-owned utilities] will measure consumption in five second increments and transmit the data back to the utility daily or on demand.”)

<sup>7</sup> *Kyllo v. United States*, 533 U.S. 27, 38 (2001).

activities that signal information about personal behavior.<sup>8</sup> As a result, information collected by the Smart Grid is valuable for many purposes other than energy efficiency, most prominently commercial exploitation by advertisers and marketers, access by criminals who wish to peek into homes, and access to household information and surveillance by government agencies.

Put simply, existing Smart Grid technologies can reveal a great deal of information about in-home activities, and these technologies are on a course to generate more detailed and voluminous data. Nonetheless, deployment is proceeding in the absence of a national process to address these risks.

Under the existing, fragmented regulatory framework, privacy protections for home energy usage data depend heavily upon what kind of entity possesses it. A utility, for example, might be subject to state utility commission rules and specific statutes that limit data use and disclosure.<sup>9</sup> A non-utility third party possessing the same data, on the other hand, probably would not face the same obligations, though general prohibitions against unfair or deceptive data practices (e.g., FTC Act § 5) and state security breach notification laws would apply.

Since individuals' privacy interests lie in what the data may reveal about them, rather than what type of entity possesses it, OSTP should promote principles that apply to all Smart Grid entities, including the activities of utility companies, third party service providers such as Microsoft and Google, and device manufacturers such as General Electric and Honeywell. Privacy principles should not subject different entities to different sets of rules where the entities are similarly interacting with consumer data. Privacy principles must also take into account the unique sensitivity of home energy usage data.

As we noted above, and as has been discussed at length elsewhere,<sup>10</sup> the privacy issues associated with home energy usage data can and should be addressed through robust application

---

<sup>8</sup> Jack I. Lerner and Deirdre K. Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3.

<sup>9</sup> See, e.g., CAL. PUB. UTILS. CODE § 394.4 (requiring electric service providers to keep "customer information"—which encompasses "customer specific billing, credit, or usage information"—confidential unless the customer gives written consent to disclosure); Cal. Pub. Utils. Comm'n, Opinion Adopting Standards of Conduct Between Utilities and Their Affiliates, Decision 97-12-088 (Dec. 16, 1997) App. A IV.A, at [ftp://ftp.cpuc.ca.gov/gopher-data/energy\\_division/affiliate/R9704011-Appendix%20A.doc](ftp://ftp.cpuc.ca.gov/gopher-data/energy_division/affiliate/R9704011-Appendix%20A.doc) ("A utility shall provide customer information to its affiliates and unaffiliated entities on a strictly non-discriminatory basis, and only with prior affirmative customer written consent."); Southern California Edison, Rule 22 (Direct Access Rules) C.3.a (Oct. 4, 2001), at <http://www.sce.com/NR/sc3/tm2/pdf/Rule22.pdf> (requiring a customer to give written authorization for a utility to disclose usage data to direct access service providers); San Diego Gas & Elec. Rule 25 (Direct Access Rules) C.3.a (Mar. 1, 1999), at [http://www.sdge.com/tm2/pdf/ELEC\\_ELEC-RULES\\_ERULE25.pdf](http://www.sdge.com/tm2/pdf/ELEC_ELEC-RULES_ERULE25.pdf) (same); Pacific Gas & Elec., Rule 22 (Direct Access Rules) C.3.a (Dec. 1, 1997), at [http://www.pge.com/tariffs/tm2/pdf/ELEC\\_RULES\\_22.pdf](http://www.pge.com/tariffs/tm2/pdf/ELEC_RULES_22.pdf) (same).

<sup>10</sup> See Comments of the Center for Democracy & Technology on Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security and Requirements, National Institute of Standards

of the full set of Fair Information Practice principles (FIPs). These principles reflect international guidelines, and go beyond the currently dominant—and discredited<sup>11</sup>—model of “notice and choice.” A recent and comprehensive definition of FIPs was set forth by the Department of Homeland Security in its Privacy Policy Guidance Memorandum.<sup>12</sup> Developed to guide homeland security projects, the DHS formulation of the FIPs is surely adequate for issues associated with the Smart Grid. Based on that DHS guidance, we recommend the following privacy framework for the Smart Grid:

- **Transparency:** Smart Grid entities should be transparent and should provide meaningful, clear, full notice to the individual regarding the collection, use, dissemination, and maintenance of home energy usage data.
- **Individual Participation:** Entities should involve the individual in the process when using energy information and, to the extent practicable, seek ratepayer consent for the collection, use, dissemination, and maintenance of home energy usage data. Entities should also provide mechanisms for appropriate access, correction, and redress regarding their use of home energy usage data.
- **Purpose Specification.** Entities that receive home energy usage data should clearly and specifically describe how they will use the data, and whether and how any other entities will use it.
- **Data Minimization.** As NIST writes in its current draft cybersecurity framework, utilities should collect the “minimum amount of data necessary for service, provision and billing.”<sup>13</sup> Only data directly relevant and necessary to accomplish a specified purpose should be collected and data should only be retained for as long as necessary to fulfill the specified purpose.
- **Use Limitation.** Home energy usage data should be used solely for the purposes specified in the notice of purpose.
- **Data Quality and Integrity; Access and Correction.** Companies should, to the extent practicable, ensure that home energy usage data is accurate, relevant, timely and

---

and Technology (Dec. 1, 2009) *available at*

<http://www.cdt.org/files/pdfs/CDT%20Comment%20NISTIR%207628%20Draft%2012-02-09%20FINAL%20-%20updated.pdf>.

<sup>11</sup> For example, National Telecommunications and Information Administration Associate Director for Domestic Policy Daniel J. Weitzner recently stated “[t]here are essentially no defenders anymore of the pure notice-and-choice model.” See Steve Lohr, *Redrawing the Route to Online Privacy*, N.Y. TIMES, Feb. 28, 2010, at Bus. 4, <http://www.nytimes.com/2010/02/28/technology/internet/28unbox.html> (quoting Mr. Weitzner).

<sup>12</sup> Issued Dec. 28, 2008, at

[http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_policyguide\\_2008-01.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf).

<sup>13</sup> NIST, *Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements*, *supra* note 3, at 106.

complete. Consumers should be able to view and correct any profiles that utilities or third parties create from their energy usage.

- **Security.** Companies should protect home energy usage data from accidental disclosure as well as malicious efforts to intercept or corrupt it. Making technical protections for data integrity and confidentiality part of the design of Smart Grid components will protect privacy and promote the security of the electric grid as a whole.
- **Accountability and Auditing .** Companies should be accountable for complying with these principles, should prevent and detect violations of an entity's policy, and should hold the responsible persons accountable. Training for personnel who handle home energy usage data may help to prevent privacy violations. In additions, audits of actual data use will help to deter and detect misbehavior.

Given that Smart Grid technology is nascent, and that its course is uncertain, the flexibility in these principles is a considerable virtue. But it also means that ongoing policy development and guidance by OSTP, NIST, and other federal agencies is necessary. Federal agencies could provide a forum for analyzing and addressing home energy usage data privacy risks, sparing stakeholders the expensive of multiple state-level proceedings.

### **C. Supporting Innovation in the Smart Grid through Home Energy Usage Data**

All stakeholders have an interest in ensuring that home energy usage data supports national Smart Grid policy goals, such as developing demand response capabilities, building energy storage capacity, and integrating renewable energy sources. For this reason, assigning ownership of home energy usage data to utilities would make little sense. As participants in a rate-regulated industry under federal and state policies that promote grid modernization, utilities have a responsibility to permit innovative data uses.<sup>14</sup> Granting exclusive rights to utilities could turn them into the exclusive gatekeepers of home energy usage data, thus hindering other efforts to use this data in Smart Grid technologies.

#### **OSTP Question 2: Should individual consumers and their authorized third-party service providers have the right to access energy usage data directly from the meter?**

Yes. Provided that it is technically feasible and safe and does not pose unacceptable risks to the trustworthiness of the grid (as determined under uniform, objective criteria administered by a neutral decision maker<sup>15</sup>), consumers and the third parties they authorize should be able to

---

<sup>14</sup> See Cal. Pub. Utils. Comm'n, Opinion Adopting Standards of Conduct Between Utilities and Their Affiliates, *supra* note 9, at App A IV.A (requiring a utility to provide customer information "to its affiliates and unaffiliated entities *on a strictly non-discriminatory basis*" upon written authorization by the customer) (emphasis added).

<sup>15</sup> A potentially useful model for this kind of determination is the set of standards for equipment that connects with the telephone network. See *generally* 47 C.F.R. part 68. A primary purpose of these "Part 68" rules "is to provide for uniform standards for the protection of the telephone

access energy usage data directly from the meter. Allowing consumers access to their home energy usage data is an important implementation of the FIPs requirements of individual participation and access, both described above.

Direct access to the meter raises two further policy issues.

First, as stated above, utilities and third parties should handle home energy usage data in a manner consistent with a comprehensive set of FIPs. Consumers have strong privacy interests in this data because it can reveal significant details about activities within the home. Whether data is disclosed to a utility, a third party via a utility, or directly to a third party, applying comprehensive and generally applicable fair information practice principles, as discussed above, will provide individuals with a predictable, consistent baseline of protection.

Second, individuals and authorized third parties should be able to access data in a useful format. The data should be made available in a non-proprietary, machine-readable, machine-processable format. Satisfying this requirement does not necessarily mean writing a standard for data interchange. If the structure and meaning of data from the meter are made publicly available and are not encumbered by patent or other restrictions, then all stakeholders will be able to make the best use of it. When accompanied by clear rules and an open process for identifying and assessing any safety or reliability risks that new devices might pose, opening data to individuals and authorized third parties will protect innovation and favor interoperability in smart devices.

**OSTP Question 3: If the smart meter, via the utility network, is the primary gateway for obtaining residential energy usage data, will it be technically and commercially feasible for consumers and their authorized third-party service providers to access the data easily and in real time?**

The question of whether it is technically and commercially feasible to provide real-time access to consumers and third-party service providers is beyond the scope of our expertise. However, one aim of Smart Grid deployment should be to ensure such accessibility. Choices about data formats and interfaces, among others, will determine the feasibility of access. Therefore, as a procedural matter, we recommend that OSTP undertake a more extensive effort to answer this question than is possible in the current proceeding. OSTP should commission an independent assessment of smart meters that are deployed or at an advanced state of development. This assessment would provide OSTP, NIST and other federal agencies, as well as state utility commissions with a comprehensive picture of smart meter architecture as it affects consumer access.

---

network from harms caused by the connection of terminal equipment and associated wiring thereto.” *Id.* § 68.1.

**OSTP Question 4: What types of policies are needed to gain consumer confidence that personal energy usage data is secure and not subject to abuse?**

As our responses to Questions 1 and 2 indicate, establishing robust, FIPs-based principles for information acquisition, use, and disclosure that apply to all Smart Grid stakeholders is critical to building the confidence that is necessary to spur consumers to adopt Smart Grid technologies and to participate in Smart Grid programs.

To be sure, a variety of federal and state laws and policies provide some assurance for consumers' privacy and security interests in household energy data. These laws include:

- The FTC Act, which prohibits “unfair or deceptive acts or practices.”<sup>16</sup> The FTC has taken enforcement actions against companies that fail to take reasonable measures to keep customer-related information secure.
- The Computer Fraud and Abuse Act (CFAA)<sup>17</sup> prohibits gaining unauthorized access to computers (which would include smart meters) that are used in interstate commerce.
- The Electronic Communications Privacy Act (ECPA)<sup>18</sup> prohibits the interception of electronic communications in transit, as well the unauthorized disclosure of stored communications contents and records. ECPA imposes few constraints on data within an organization, however, and thus fails to address an important class of privacy risks in home energy usage data.
- Security breach notification laws are state-level statutes that generally require any person or organization that controls personally identifiable information to report instances of unauthorized access.<sup>19</sup>

Even taken together, however, these laws do not provide adequate privacy and security assurances, for two reasons.

First, it is not yet clear whether, and if so how, some of these protections will apply to the Smart Grid. The standards for law enforcement or civil litigant access to home energy usage data—critical privacy questions—are unclear and under current law are likely to vary based on the location and entity holding the data, as well as state by state.<sup>20</sup> Is it permissible for the

---

<sup>16</sup> 15 U.S.C. § 45.

<sup>17</sup> 18 U.S.C. § 1030. Most states have analogous “anti-hacking” statutes.

<sup>18</sup> 18 U.S.C. §§ 2510-22, 2701-2712, 3121-27.

<sup>19</sup> Forty-five states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted security breach notification laws. Nat'l Conf. of State Legislatures, State Security Breach Notification Laws (Dec. 9, 2009), at <http://www.ncsl.org/default.aspx?tabid=13489> (providing links to statutes).

<sup>20</sup> Jack I. Lerner and Deirdre K. Mulligan, Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home, 2008 Stan. Tech. L. Rev. 3 (discussing bizarre implication of easy access to utility records due to 4<sup>th</sup> Amendment business records doctrine

National Security Agency or another government agency to ask a utility to divert all of the smart grid data—information that reveals the in-home activities of millions of individuals—to a secret room for mining and analysis? Nothing in current statutory law clearly prohibits this. Clearly, laws about government access must be updated to clarify when, if ever, and under what circumstances such highly intrusive data may be accessible to the government. Further, Smart Grid technologies are nascent. None of the Smart Grid stakeholders fully understands the scale and scope of energy usage data that may be generated, how it could be combined with other data sources, and what might be inferred through analysis.

Second, the legal frameworks outlined above are largely reactive and provide little incentive to include privacy controls in the design of smart meters and other Smart Grid components. For example, the Computer Fraud and Abuse Act provides criminal and civil penalties for individuals who cause harm by hacking into computers (such as smart meters) irrespective of the adequacy of technical protections on the system in question. Thus, it provides no additional incentive to device manufacturers, utilities, and other service providers to invest in security.

OSTP's support for the privacy principles discussed in this comment would go a long way toward promoting a uniform, comprehensive framework that will provide guidance for federal agencies, state utility regulators, and technology firms. Adopting a "privacy by design" approach, and promoting principles and standards that reflect privacy interests during buildout, rather than attempting to tack on privacy at a later point, is the most effective means of protecting consumer privacy and security.<sup>21</sup> Embedding privacy protections into the technology and business practices now, before smart meters and other Smart Grid technologies are fully deployed, will also be less expensive than attempting to address these issues in the future, and will make the grid more adaptable to changing threats to privacy and security as use increases.

For these reasons, we urge OSTP to promote guidelines or best practices based on FIPs for all entities engaged in the collection and use of home energy usage data.

#### **A Note on Process.**

As noted, we applaud both OSTP and NIST for engaging with the public to understand its views on Smart Grid deployment and the surrounding policy questions. Energy infrastructure and energy independence are critical societal issues, and it is right to address them in a public forum that is user-friendly and open to all.

At the same time, however, the process instituted by OSTP—with very little notice of the process overall, essentially no guidance on what OSTP or NIST plans to do with the information

---

versus warrant requirement under *Kyllo v. United States*, 533 U.S. 27 (2001) to derive essentially the same information about in-home energy consumption, reviewing state case law regarding law enforcement access to utility records and discussing privacy provisions of utility law in California).

<sup>21</sup> See Information and Privacy Commissioner of Ontario, *Privacy by Design*, <http://www.privacybydesign.ca/>.

received, and extremely short timelines for response (for example, the comment period for questions on data access and ownership spanned only four business days)—creates profound difficulties for public interest groups and members of the public who wish to participate. In many cases, it is probably impossible for such groups and individuals, who have neither endless resources nor concentrated interests, to fully participate. Even those with resources and concentrated interests have struggled to participate. For example, Southern California Edison felt the need to request an extension in a proceeding on similar issues before the California Public Utilities Commission in order to focus on this proceeding, and was supported by Walmart and the California Energy Storage Alliance.

We urge OSTP to recognize that appropriate information gathering and policy development related to the Smart Grid requires a considered and ongoing effort, with full participation by all affected parties. We request that OSTP revise its processes to reflect these considerations.

Sincerely,

/s/

Aaron J. Burstein\*  
University of California  
School of Information  
Berkeley, CA 94720

/s/

Deirdre K. Mulligan\*  
University of California  
School of Information  
Berkeley, CA 94720

/s/

Jennifer M. Urban  
Samuelson Law Technology  
& Public Policy Clinic, for:  
James X. Dempsey  
Ari Schwartz  
Center for Democracy & Technology

---

\* Affiliations for these authors are provided for purposes of identification only. The views expressed in this comment do not purport to represent those of the University of California.