BEFORE THE PUBLIC UTILITIES COMMISSION OF THE

STATE OF CALIFORNIA

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	Rulemaking 08-12-009 (Filed December 18, 2008)

JOINT COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY AND THE ELECTRONIC FRONTIER FOUNDATION ON PROPOSED POLICIES AND FINDINGS PERTAINING TO THE SMART GRID

JENNIFER LYNCH, Attorney[1]
Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7515
Attorney for CENTER FOR DEMOCRACY & TECHNOLOGY

LEE TIEN, Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333 x102
Attorney for ELECTRONIC FRONTIER FOUNDATION

Dated: March 9, 2010

[1] Berkeley Law students Jonas Herrell, David Marty, and Shane Witnov, along with School of Information Masters Candidate, Longhao Wang, participated in the drafting of these comments.

BEFORE THE PUBLIC UTILITIES COMMISSION OF THE

STATE OF CALIFORNIA

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	Rulemaking 08-12-009 (Filed December 18, 2008)

JOINT COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY AND THE ELECTRONIC FRONTIER FOUNDATION ON PROPOSED POLICIES AND FINDINGS PERTAINING TO THE SMART GRID

I. Introduction

The Center for Democracy & Technology ("CDT") and the Electronic Frontier Foundation ("EFF") file these joint comments in response to the Assigned Commissioner and Administrative Law Judge's Joint Ruling Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid, issued February 8, 2010 ("Joint Ruling"). CDT and EFF thank the Commission for the opportunity to submit comments discussing these important questions and commend the Commission's initiative on the matters to date.

The Center for Democracy & Technology is a non-profit, public interest organization with broad experience and expertise in matters of consumer privacy and emerging technologies. CDT has offices in Washington, DC and San Francisco, California. EFF is a non-profit member-supported organization based in San Francisco, California, that works to protect free speech and privacy rights in an age of increasingly sophisticated technology.

In addressing the issues raised by the Joint Ruling, we recommend the following:

- Privacy concerns raised by data collection within the Smart Grid require regulatory action on the part of the Commission. (*See Section II)*
- The Commission's authority to regulate consumer privacy and data access issues on the Smart Grid is derived from the California Constitution, Senate Bill 17, and the Commission's past decisions. (*See Section III*)
- The Commission should define the scope of customer energy data that warrants privacy protection. (*See Section IV)*
- The Commission should adopt privacy and security principles based on the Fair Information Practice principles (FIPs) to ensure that Smart Grid proposals will provide the privacy protections required by state and federal law. (*See Section V*)
- To fulfill the requirements of Senate Bill 17, the Commission should require utilities to employ Fair Information Practice principles as part of their Smart Grid deployment plans. (*See Section VI*)
- The Commission should consider and adopt our recommended modification to the Proposed Access Rule, as provided in our Appendix A. (*See Section VII*)
- The Commission should include privacy-related quantitative metrics for Smart Grid implementations. (*See Section VIII*)
- The Commission should not wait for privacy standards from the national standard setting bodies, and should adopt the Fair Information Practice principles now. (*See Section IX*)

We hope that our comments and recommendations here will both advance the Commission's understanding of the important privacy interests that are at stake in these proceedings and provide useful guidance to the Commission as it seeks compliance with the requirements and mandates of State Senate Bill 17, the Federal Energy Independence and Security Act of 2007, and the California Constitution.

II. Privacy Concerns Raised By Data Collection within the Smart Grid Require Regulatory Action on the Part of the Commission

A. Data Flows Enabled by Smart Grid Technology Represent a Profound Shift in the Customer-to-Utility Relationship

The Smart Grid promises great benefits to consumers and the environment, including lowered energy costs, increased usage of environmentally friendly power sources, and enhanced security against attack and outage. At the same time, however, the Smart Grid presents new privacy threats through its enhanced collection and transmission of detailed consumption data – data that can reveal intimate details about activities within the home and that can easily be transmitted from one party to another. The following aspects of these expanded data flows represent a profound shift from the traditional customer-to-utility relationship:

> **(1) Granularity of Usage Information:** The Smart Grid entails collection of much more detailed data about consumer energy consumption than previous technologies allowed. 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 this data at much shorter time intervals—down to real-time or near real-time intervals. The emergence of increasingly sophisticated metering technologies is enabling the unprecedented collection of energy consumption data—from 750 to 3,000 (or more) data points a month— and will reveal variations in consumption that can reflect specific household activities such as sleep, work, and travel habits.[2]
>
> **(2) New Types of Information:** Smart Grid technologies collect a much greater variety of information than has been collected by conventional energy services. In addition to detailed energy consumption data, utilities may collect distributed generation data, unique identifiers and functionality of home appliances, temperature inside the home, and location information of plug-in hybrid electric vehicles, just to name a few. And this is only the raw data. With this data in

[2] 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 (2008).

hand, it becomes trivial to infer presence and absence in the home, sleep schedules, and other highly personal routines.[3]

(3) Third Party Incentives and Access: The sheer volume of granular data provided by Smart Grid technologies, combined with its revealing nature, will make it highly attractive to a number of parties other than the utilities themselves, including marketers, law enforcement or other government actors, civil litigants, and criminals,[4] The attraction for marketers, for example, has already created an emerging market in consumer energy data. Within the new Smart Grid, third-party, non-utility operations will have unprecedented incentives to gain access to customer data. Beyond direct access to data held at utilities, third parties will seek to use utilities as conduits for customer information or will market devices that pull customer data directly from within the home, bypassing the utility's equipment.

The challenge for the Commission is to develop rules that both protect the consumer against misuse of this data and empower the consumer to access this data, use it and share it with entities other than the utility as they offer new and useful services to consumers.

B. New Technologies and Services Create Attendant Privacy Risks

New energy services that allow consumers access to their own detailed usage data present potential benefits in terms of energy efficiency and reliability. Yet these services will allow entities other than utilities to receive consumer energy consumption data and use it in new ways. This profound shift in the data flow away from the traditional consumer-to-utility relationship challenges key assumptions underlying existing privacy laws and regulations.

Further, the emergence of increasingly sophisticated metering technologies, which enable the unprecedented collection of energy consumption data, will remove a "latent structural limitation" that previously protected the revelation of intimate details about household activities.[5]

---

[3] Mikhail Lisovich, Deirdre Mulligan, & Stephen Wicker, *Inferring Personal Information from Demand-Response Systems*, IEEE Security & Privacy, Jan.-Feb. 2010, at 11-20.
[4] *See* § II.B, *infra*.
[5] *See* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. Rev. 1605, 1626 (2007) (noting how "the widespread diffusion of an emerging technology effectively causes a rights-shift with respect to privacy interests protected by latent structural constraints.").

For example, new non-intrusive appliance load monitoring ("NALM") techniques make it easy to reconstruct information about energy consumption of individual appliances from a household's aggregate smart meter data,[6] and researchers have already compiled libraries of appliance load signatures.[7] Research shows that analyzing fifteen-minute interval aggregate household energy usage data can by itself pinpoint the use of most major home appliances.[8] As the time intervals between data collection points decrease, home appliance use will be inferable from overall utility usage data with greater and greater accuracy.[9]

Activities that might be revealed through analysis of home appliance use data include personal sleep and work habits, cooking and eating schedules, the presence of certain medical equipment and other specialized devices, presence or absence of persons in the home, and activities that might seem to signal illegal, or simply unorthodox, behavior.[10] As a result, information collected by the Smart Grid becomes highly valuable for many purposes other than energy efficiency, most prominently: commercial exploitation by advertisers and marketers, household surveillance by law enforcement, and access by criminals attempting to break into homes or commit identity theft.

1. Commercial Interests in Acquiring Customer Energy Data Create Privacy Risks

Because of the intimacy of home life, data collected by Smart Grid technologies and services could be used for purposes especially contrary to consumer interests and expectations. For example, an analysis of smart meter data revealing customers' home activities and daily routines could be commercially valuable to life insurance companies looking to adjust rates for customers with purportedly unhealthy lifestyles. Financial institutions making home mortgage loans might also be interested in their customers' energy usage records to verify whether the customers are actually living in those houses. Advertising companies offering behavioral

---

[6] Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies* app. A at A-1 (2009), *available at* http://ssrn.com/abstract=1462285.

[7] *Id*. at 2. The construction of load pattern libraries can be manually crafted, or generated by machine learning algorithms such as a neutral network.

[8] Research suggests this can be done with accuracy rates of over 90 percent. *See* Elias Leake Quinn, *Privacy and the New Energy Infrastructure* 28 (2009), *available at* http://ssrn.com/abstract=1370731.

[9] California utilities are already deploying smart meters that are capable of taking usage readings every five seconds. *See* Calif. Energy Comm'n, CEC-400-2008-027-CT, *Proposed Load Management Standards* 25 (Draft Comm. Report, 2008), *available at* http://www.energy.ca.gov/2008publications/CEC-400-2008-027/CEC-400-2008-027-CTD.PDF.

[10] Lerner & Mulligan, *supra* note 2.

targeting products might wish to enhance existing customer profiles with energy usage data that reveals customer activities and habits, following a recent trend in the merging of online and offline data sources to enhance targeted third-party advertising.[11]

2. Government Agency Incentives to Acquire Customer Energy Data Create Privacy Risks

The detailed and revealing nature of Smart Grid data also will be valuable for surveillance by government agencies. For example, law enforcement agencies already use electricity consumption data. In *Kyllo v. United States*,[12] the government relied on electrical utility records to develop its case against a suspected marijuana grower.[13] Government agents issued a subpoena to the suspect's utility to obtain energy usage records and then used a utility-prepared "guide for estimating appropriate power usage relative to square footage, type of heating and accessories, and the number of people who occupy the residence" to show that the suspect's power usage was "excessive" and thus "consistent with" a marijuana-growing operation.[14] In 2004, a California family was put under surveillance by law enforcement for having an unusually high electricity bill, which turned out to merely reflect the legitimate activities of a busy household.[15] In 2000, the California Narcotic Officers' Association unsuccessfully attempted to get the Commission to overturn its previously ruling that utilities only provide customer data to law enforcement with proper legal service.[16]

As Smart Grid technologies continue to collect ever more finely-grained data about household habits, law enforcement officials will become even more interested in accessing that data to develop cases. In investigating crimes, for example, agencies may want to establish or confirm presence at an address at a certain critical time; this information may be gleaned from smart meter reading data or temperature inside the home collected by a programmable thermostat.

---

[11] For more about recent trends in data aggregation and the development of enhanced customer profiles for advertising purposes, see CDT, *CDT's Guide to Behavioral Advertising*, http://cdt.org/privacy/targeting/.
[12] 533 U.S. 27 (2001).
[13] *Id*. at 30.
[14] *United States v. Kyllo*, 809 F. Supp. 787, 790 (D. Or. 1992), *aff'd*, 190 F.3d 1041 (9th Cir. 1999), *rev'd*, 533 U.S. 27 (2001).
[15] Jo Moreland, *Drug Raid Has Carlsbad Family Seeing Red*, N. County Times, Mar. 25, 2004, *available at* http://www.nctimes.com/news/local/article_ea2047e8-59e1-551e-b173-ce89ffad4d90.html.
[16] D.01-07-032 at 1.

While Smart Grid data certainly may be useful for these purposes, the privacy implications of law enforcement access, especially in the traditionally protected area of the home, call for strong, constitutionally adequate protections for this information, careful procedures on the part of utilities and others with access to this data, and technology design that allows for strong data protection.

3. Civil Litigants' Incentives to Acquire Customer Energy Data Create Privacy Risks

Civil litigants may also place a high value on detailed energy usage data. For instance, an insurance company contesting a homeowner's claim might seek access to the homeowner's energy data to disprove that he actually owned the specific appliances he claimed. Similarly, in a custody proceeding, a spouse may seek energy data to show the other spouse took the children out of the state for two days without proper consent. In both cases, the detailed usage data would certainly be relevant to proving or disproving the contested fact. As with access by government agencies, effective procedural protections should be required, as should careful procedures for managing civil requests on the part of utilities and other providers. These include first requiring litigants to seek data from the customer directly (who, under our recommendations, should have access to data pertaining to his or her home energy usage). If the only way to obtain the information is directly from a regulable entity, then the litigant should be required to show a compelling interest in the information, and the entity should provide energy customers with notice and an opportunity to object before disclosing data.

4. Criminal Incentives to Acquire Customer Energy Data Create Privacy Risks

Criminals might also seek access to smart meter data or other information collected by the Smart Grid, in hopes of using this data to infer whether anybody is present in a house and to determine the most desirable time to commit a crime. In addition, because the Smart Grid enables the accumulation of personally identifiable and other revealing information over long periods of time, information-gathering via Smart Grid technologies could reveal behavior patterns likely to be repeated in the future, allowing criminals to plan for future crimes. The information could also be used by criminals to commit identity theft, especially if utilities or other providers use unsecured paths to transmit data. For instance, many utilities use energy

consumption data to authenticate customers, making the information particularly valuable to those attempting illicitly to take over someone else's account.[17] Failing to encrypt data transmission within the Smart Grid compounds these threats to customer data security.

C. Current Privacy Legal Frameworks Offer Some Protections for Energy Data But Are Insufficient to Fully Protect Data in the Smart Grid

The significant privacy risks to consumers, described above, are compounded by the dearth of clear rules that apply to the new technology landscape. As the National Institute of Standards and Technology (NIST) noted in its First Draft 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."[18]

In this proceeding, the Commission has been presented with the important opportunity and responsibility[19] to develop privacy protections for California citizens' energy data. Both the California and Federal Constitutions, as well as various regulatory decisions and provisions, provide some protections for energy data, but these protections were not designed to cover the unprecedented volume of data, nor varieties of new data, that the Smart Grid will make available about household activities. As such, these protections need to be supplemented to ensure that Californians can continue to enjoy the level of privacy they expect and are entitled to in their homes.

Historically, the principal source of privacy regulation for electricity data has been state public utility commissions, which place varying restrictions on disclosure of consumer energy data.[20] Generally, state utility commissions are just beginning to consider the privacy implications of Smart Grid data, putting California in a leadership position.[21] Because the

---

[17] For instance, San Diego Gas and Electric (SDGE) uses the amount of the last SDGE bill to authenticate its customers when the customers sign up for an online account. *See* SDGE*, My Account*, https://myaccount.sdge.com/myAccountUserManager/pageflows/usermanager/Registration/begin.do.

[18] Nat'l Inst. of Standards & Tech., *Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements* (2009), *available at* http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf.

[19] *See, e.g.*, D.09-12-046 at 26 (finding that the Commission should create rules about privacy and security to protect customers); D.90-12-121 at 11 (holding that utilities can only provide data to law enforcement pursuant to legal process).

[20] Quinn, *supra* note 6, at 24.

[21] For example, the National Association of Regulatory Utility Commissioners (NARUC) will consider a resolution in 2010 that would encourage member states to support several regulatory protections on consumer data collected in

existing laws alone do not provide adequate protection for the categories and quantities of data that the Smart Grid will generate, the Commission should use its regulatory authority to ensure that the Smart Grid does not undermine the privacy protections guaranteed to California citizens.

Specifically, as we describe in later sections, the Commission should (1) define the scope of customer energy data that warrants privacy protection, (2) broadly adopt cyber security and privacy principles to ensure that smart grid proposals will provide sufficient privacy protections, (3) require utilities to employ Fair Information Practice principles (FIPs) as part of Smart Grid deployment plans, (4) provide additional privacy protections in the Proposed Access Rule, (5) request privacy-related quantitative metrics from utilities in smart grid implementations, and finally, (6) the Commission should not wait for privacy standards from the national standard-setting bodies, but should adopt FIPs immediately.

III. The Commission's Authority to Regulate Consumer Privacy and Data Access Issues on the Smart Grid Is Derived from the California Constitution, Senate Bill 17 and the Commission's Past Decisions

The Commission stated its policy objective in D.09-12-046 to "[e]nsure all information is secure and that a customer's privacy is protected."[22] It further stated it would require utilities put in place "sufficient privacy and security measures . . . to mitigate the potential for fraud and hacking" and that "access to usage data must be provided consistent with the rules [the Commission] adopt[s] to ensure that access is provided consistent with EISA, the general public interest, and state privacy rules."[23]

The California Constitution's privacy provision,[24] along with Senate Bill 17,[25] support these goals and provide the Commission with broad authority to adopt rules and protocols designed to protect and preserve consumer privacy rights. We discuss these and additional grounds for the Commission's authority in this section.

---

the Smart Grid. *See* NARUC, *Draft Resolutions Proposed for Consideration at the 2009 Annual Convention of NARUC* 14-17 (2009), *available at* http://annual.narucmeetings.org/09_1106_Proposed_Resolutions.pdf; *see also* Nat'l Inst. of Standards & Tech., *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0*, at 84 (2009), *available at* http://www.nist.gov/public_affairs/releases/smartgrid_interoperability.pdf.

[22] D.09-12-046.

[23] *Id.*

[24] Cal. Const. art. I, § 1.

[25] Specifically Cal. Pub. Util. Code §§ 8360(i), (j).

In *White v. Davis*[26] the California Supreme Court explained that "the moving force" behind California's constitutional right to privacy "was a more focused privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society," and that its "primary purpose is to afford individuals some measure of protection against this most modern threat to personal privacy."[27]

Importantly, our state constitutional privacy right protects Californians against private businesses as well as the government. As the *White* court put it, the right "prevents government and business interests from collecting and stockpiling unnecessary information about us," partly because "[t]he proliferation of government and business records over which we have no control limits our ability to control our personal lives."[28] Thus, among the "principal 'mischiefs'" targeted by the constitutional right are "the overbroad collection and retention of unnecessary personal information by government and business interests" and "the improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party."[29]

The Commission has recognized its constitutional obligations to protect privacy in past decisions. When confronted with the consumer privacy concerns presented by telephone monitoring technologies, in Decision No. 88232, the Commission unequivocally stated that, "[o]ur constitutional responsibilities and those of the utilities we regulate, are paramount. . . ."[30] In *The Matter of the Application of Pacific Bell,* when confronted with the consumer privacy concerns presented by Pacific Bell's default installation of caller identification technology, the Commission drew upon its constitutionally granted authorities and rightly refused to allow commercial expediency to take precedent over the rights of California citizens. It stated:

> If the service is to be offered consistently with constitutional guarantees and the public interest, it must be offered in a way that maximizes the ease and freedom with which California citizens may choose not to disclose their calling party numbers. We will not compromise an individual's free exercise of his or her right of privacy in order to place in the hands of the Caller ID subscriber a more valuable mailing list, a marginally better

[26] *White v. Davis*, 13 Cal.3d 757 (1975).
[27] *Id*. at 774.
[28] *Id*.
[29] *Id*. at 775.
[30] *In re PT&T Co.*, 83 C.P.U.C. 149 (1977).

> method of screening or managing telephone calls, or even a slightly more effective deterrent to unlawful or abusive uses of the telephone.[31]

Smart Grid technology poses far greater, yet far less visible, threats to consumer privacy than Caller ID. Unlike Caller ID, which only transmits the caller's phone number, Smart Grid technologies can reveal minute details about the lives in a household. This suggests even greater reason for the Commission to address these issues. Further, these precedents strongly support interpreting the Commission's constitutional obligations to include protecting consumers from the full range of privacy threats.

California State Senate Bill 17 (Padilla), which added sections 8360 through 8369 to the California Public Utility Code, also provides the requisite authority to protect consumer privacy. Specifically, section 8360(i) requires that the Commission "[d]evelop standards for communication and interoperability of appliances and equipment connected to the electric grid."[32] The Commission is empowered to regulate the privacy and security of consumer energy data because such privacy and security are critical aspects of any "standards for communication." Likewise in section 8360(j), the legislature has tasked the Commission with "[i]dentifying and lowering [ ] unreasonable or unnecessary barriers to adoption of smart grid technologies, practices, and services." Because customers will be dissuaded from adopting Smart Grid technologies unless the risk to privacy posed by such technologies is addressed, the Commission can and should use its authority under section 8360 to create consumer privacy protections, thus lowering resistance to adoption.

IV. The Commission Should Define the Scope of Customer Data that Warrants Privacy Protection

Designing an effective framework to protect customer data requires a specific articulation of what information requires protection. We recommend that the Commission adopt a robust and expanded interpretation of the term "customer information" to account for the new types of information on the Smart Grid. The Commission should then act to regulate the collection, use, and dissemination of that customer information as we describe in subsequent sections.

[31] *In re Pacific Bell*, 44 C.P.U.C.2d 694 (1992).
[32] Cal. Pub. Util. Code § 8360(i).

The California Public Utility Code currently describes "customer information" in section 394.4 as including "customer specific billing, credit, or usage information."[33] This section importantly requires Electric Service Providers to treat such information as confidential unless the customer consents otherwise in writing.[34] Affiliate Transaction Rule IV.A similarly articulates the confidentiality requirement that attaches to customer information, in this case, when the information is in the hands of the utilities.[35] The rule provides that: 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.*[36]

"Customer information" should be construed to cover the broad set of intimate information that is now collectable within the Smart Grid and should apply to all entities collecting, storing or transmitting customer data. We suggest that, beyond its current denotation, the term be expressly interpreted to include all usage data and device data capable of revealing either personally identifiable information or household-identifiable information.[37] Specifically, the Commission should expressly interpret the meaning of "customer information" to include:

> (1) *traditional personally identifiable information* (PII), such as account information used for billing purposes and unique device identifiers tied to an individual name, which is either immediately personally identifiable or becomes personally identifiable when combined with other collected information;
>
> (2) *data collected about an individual household* in the Smart Grid that is revealing of home life by itself or when analyzed or combined with other information. Examples of this second category of data include, without limitation: granular usage data from individual households, records of plug-in hybrid electric vehicle (PHEV) use, and specific metering and device data (e.g. thermostat temperature); and

[33] *See* Cal. Pub. Util. Code § 394.4(a) ("Customer information shall be confidential unless the customer consents in writing. This shall encompass confidentiality of customer specific billing, credit, or usage information.").
[34] *See id.*
[35] D.97-12-088, app. A, Rule IV.A, *rev'd by* D.98-08-035, *amended by* D.98-12-075.
[36] *Id.* (emphasis added).
[37] This distinction between personal identifiability and household identifiability is intended to emphasize the importance of protecting the privacy of households, in addition to the privacy of individual persons. We focus here on protections that the home and household deserve, but we note that the energy usage data of organizations such as churches, political associations, and medical offices may warrant similarly strong protections.

(3) *energy usage data collected from the home by entities without the permission or intervention of the utility*, to the extent that the authority of the Commission covers such entities.

Sometimes information in the second category will be personally identifiable when combined with other types of information or when the number of people in a household is small. Regardless of whether it is individually identifiable, however, household-identifiable information is inherently revealing of household activities and home life, traditionally private domains that are, and should continue to be, protected from observation. It can still reveal highly personal and invasive details about daily activities of people living in the home, such as the use of a specific medical device or an absence from the home, raising serious privacy issues. Further, given that 32.2 million people live alone in the U.S. and twenty eight percent of American households have single-person occupancy,[38] household-identifiable information is functionally equivalent to "personally identifiable information" for a significant number of consumers.

The principles discussed here for customer information outline the minimum protections required for this basic category of data. Some of the information included within the customer information, such as PII and location-identifying information, will require additional protections.

V. The Commission Should Adopt Privacy and Security Principles Based on the Fair Information Practice Principles (FIPs) to Ensure that Smart Grid Proposals Will Provide the Privacy Protections Required by State and Federal Law

In section 5.5 of the Joint Ruling, the Commission asks broadly what cyber security and privacy principles Smart Grid proposals should meet.[39] As has also been discussed at length elsewhere,[40] the privacy issues associated with home energy usage data can and should be addressed through robust application of the full set of FIPs. We strongly urge the Commission to use the FIPs as a general overarching framework to guide the privacy principles and rules it adopts. These principles reflect international guidelines, and go beyond the currently dominant—

[38] U.S. Census Bureau, *Facts for Features: Unmarried and Single Americans Week*, July 21, 2009, http://www.census.gov/Press-Release/www/releases/archives/facts_for_features_special_editions/014004.html.
[39] *Assigned Commissioner and Administrative Law Judge's Joint Ruling Amending Scoping Memo and Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid* 33-39 (Feb. 8, 2010) [hereinafter "Feb. Joint Ruling"].
[40] *See* CDT, *Comments of the Center for Democracy & Technology on Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security and Requirements, National Institute of Standards and Technology* (2009) *available at* http://www.cdt.org/files/pdfs/CDT%20Comment%20NISTIR%207628%20Draft%2012-02-09%20FINAL%20-%20updated.pdf.

and discredited[41]—model of "notice and choice." The FIPs have been used for information management since 1973 and provide a well-tested framework for balancing and harmonizing privacy concerns with other interests. They have gained broad acceptance by national and international privacy regulators and have been applied in many contexts related to consumer privacy. The FIPs are well-aligned with the requirements of SB 17. Properly formulated and rigorously implemented, the FIPs provide a broad, comprehensive privacy framework that should underlie all privacy principles for Smart Grid deployment. Adopting FIPs as a framework is an essential part of protecting consumer privacy and ensuring that the Smart Grid maximizes "benefit to ratepayers"[42] by creating a system that carefully weighs the tradeoffs between disclosure and privacy protection.

A. The Fair Information Practice Principles

The Commission should adopt the FIPs framework because it provides a complete system for considering privacy and consumer security issues. We rely here on the articulation of the FIPs recently adopted by the US Department of Homeland Security,[43] on the belief that a framework developed for information systems affecting the national security is also well-suited to the issues posed by the Smart Grid. The DHS framework includes the following eight principles: (1) Transparency, (2) Individual Participation, (3) Purpose Specification, (4) Data Minimization, (5) Use Limitation, (6) Data Quality and Integrity, (7) Security, and (8) Accountability and Auditing. These principles are described at length in this section and referred to extensively throughout our recommendations in the sections that follow.

1. **Transparency:** Data management practices should be transparent and should provide meaningful, clear, full notice to the consumer regarding the collection, use, dissemination, and maintenance of customer information.

An entity that handles customer information must make comprehensive and accurate disclosures to customers about the collection, use, dissemination and maintenance of customer

[41] 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).
[42] SB 17.
[43] *See*, U.S. Dept. of Homeland Sec., *Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

information. This disclosure must be made to the consumer prior to any collection. This information-sharing must extend beyond mere notice of collection practices; it must also include providing consumers with clear, detailed information about the specific uses of their data, retention periods, and any transfers of data to or access by other entities. Notices should state clearly: what information is collected, whether this information is shared and with whom it is shared, the period that data is retained, and the contact information for an official at each company responsible for the policy and for personal data collected by the system. Further, Smart Grid entities, including utilities, should also provide consumers with access to the personally identifying information collected about them, as well as all usage data collected about their homes. This principle aligns closely with section 8360(h), which requires that consumers be provided with "timely information and control options."[44] This principle is also essential to the successful implementation of many of the following principles, especially Individual Participation and Accountability and Auditing.

2. **Individual Participation:** Regulable entities should involve the individual in the process when they use customer information and, to the extent practicable, seek ratepayer consent for the collection, use, dissemination, and maintenance of customer information.

New smart meters create the need for regulable entities to give customers a choice about the types of customer information collected and its use, transfer, and maintenance, including retention. To fully recognize the principle of individual participation, regulable entities must respect the range of consumer preferences with respect to their data that will exist at multiple points along the data path.

Under the Public Utilities Code, customer information, including usage information, is confidential.[45] To protect consumer privacy, regulable entities should be required to get affirmative written customer consent prior to the collection and use of customer information for any secondary purposes beyond what is strictly required for the provision of service. Consumers implicitly agree to the minimum data disclosures required for utilities to provide energy generation and billing. However, any other uses that are not strictly necessary require affirmative consent. For example, affirmative written consent would be required for a utility to

[44] Cal. Pub. Util. Code § 8360(h).
[45] *Id.* § 394.4(a).

use customer information for delivering advertisements to its customers because it is not strictly necessary to the primary purpose of providing energy service.

3. **Purpose Specification:** Regulable entities should specifically articulate the purpose or purposes for which customer information will be used.

Regulable entities should provide consumers with information about how the entity will use their data *before* the time of collection. The specification of purpose should fully describe the purposes for which the data being collected will be used. These will likely include uses of customer energy data necessary for core entity operations and services, such as efficient and reliable delivery of electricity, demand response, and billing. To the extent that utilities plan to use data for purposes not strictly necessary to the performance of core operations and services, such as marketing, customers should also have sufficient opportunity to separately and expressly consent to such uses.

Clearly articulating the purpose of data use enables the consumer to make an informed choice before deciding to share data. In the context of the Smart Grid, for example, one would expect a utility to specify to a consumer that "customer information" will be used for the purposes of providing time-of-use pricing that may reflect discounted rates during certain times of the day. If a utility plans to share customer information with any third-party service providers, the utility must disclose that fact along with all uses for which the third-party will use the data. If the utility later wishes to change the purpose for which the customer information is used, the utility must first notify consumers and give them the choice whether to consent to that new use.

4. **Data Minimization:** 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.

Generally, Smart Grid standards should support, and technologies should be capable of, appropriate data minimization. The Data Minimization principle dictates that regulable entities may only collect and maintain customer data necessary for the performance of specified purposes, as defined above.[46] Unnecessary information should not be collected; as soon as collected information becomes unnecessary for a stated purpose, it should be deleted.[47]

[46] *See supra* § V.A.3.

[47] OpenADR is an example of a technology that can contribute to data minimization by significantly reducing data collection while still enabling demand response functionality. Demand Response Research Ctr., CEC-500-2009-

In addition to supporting consumers' privacy interests, data minimization is an important part of Smart Grid cyber security, which the Commission is responsible for overseeing under section 8360(b) of SB 17, and also is important to protecting customer safety as required by section 8363.[48] As previously discussed, energy data could be used for many unauthorized and sometimes malicious purposes.[49] Minimizing data collection is a powerful tool for protecting against these security and privacy threats: if the data does not exist, it cannot be compromised. Therefore, adequate minimization requirements for the data that regulable entities collect and keep will address security and privacy concerns, while leaving untouched the data that entities need to fulfill their core operations.

The initial technical architecture that regulable entities adopt to implement the Smart Grid can have a substantial impact on the long-term scope of their data collection practices. For example, collecting and aggregating usage data at the meter level (or household level) could help protect consumer privacy through data minimization. Smart meters deployed in California are already furnished with memory and processing power. The current smart meters could compute electricity bills based on time-of-use pricing, and only periodically transmit aggregate usage and billing information back to the utility, at user defined time spans such as weekly or monthly. These changes would not affect the accuracy of billing or reveal the consumer's consumption data on a granular level to the utility. Yet, all smart meters are not equally smart. When a utility installs smart meters that do not have aggregation capabilities, consumers lose their ability to choose what level of data the utility can see. Consequently, they may surrender more data than the utility actually needs.

Consumers should be provided with tools to aggregate their energy usage data at the meter level before the data is sent along. Consumers should be able to decide the frequency of aggregated smart meter data reported to regulable entities. This requirement is easily implemented because smart meters can be remotely updated, which is all that is required to implement this aggregation function. Provide consumers with tools to decide the time intervals

---

063, *CEC OpenADR-Version 1.0 Report* 1 (Pier Final Project Report, 2009) *available at* http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf (last visited Mar. 9, 2010).

[48] Cal. Pub. Util. Code §§ 8360, 8363.

[49] *See supra* § II.B.

of smart meter reading reported enables households to fully participate in the decision to share their customer information outside of the home.[50]

Residential energy management systems also can minimize data collection by regulable entities. Instead of registering individual smart devices with utilities, consumers could use residential energy management systems, under their control, to manage their devices.[51] In this architecture, smart devices only register with consumers' own residential energy management systems and are invisible to the utilities and other regulable entities who communicate directly with the residential energy management system.[52] Residential energy management systems are being actively developed by commercial entities[53] as well as researchers at University of California.[54]

Importantly, it is presently unclear whether utilities need to collect information about the functioning of individual appliances, or even individual houses, in order to implement effective load management or demand response programs. For many purposes and programs, such detailed data should not be necessary. Given the privacy interests in household-level usage data, the collection and use of it should be subject to scrutiny. Because entities seeking to collect this type of data are in the best position to demonstrate why it is needed, these entities should bear the burden of proving the need for granular customer information, and should be required to show why it is necessary for specific purposes.

The Commission should also apply the Data Minimization principle to regulable entities' data retention practices and should consider revising the current retention periods for customer records, which widely reflect the industry standard of seven years.[55] Although regulable entities may need to retain some data like billing records and load research data for longer periods of time, they should be required to destroy unrelated or unnecessary data. For example, for billing

---

[50] Minimizing the data that leaves the home is especially important because of the well-established constitutional protections for data residing in the home, as discussed, *supra*, § II.C.

[51] S. Cal. Edison, *SmartConnect Use Case: C6 - Customer Uses an Energy Management System (EMS) or In-Home Display (IHD)*, at 18 (2009), *available at* http://www.sce.com/NR/rdonlyres/C39473B2-50BF-48C6-BAC7-4904DEE0D51F/0/C6_Use_Case_090105.pdf.

[52] *Id.*

[53] Press Release, Tendril, Tendril Achieves First Open ADR Compliant Platform (Jan. 29, 2009) *available at* http://www.tendrilinc.com/2009/01/tendril-achieves-first-open-adr-compliant-platform-2/.

[54] David Auslander & Daniel Arnold, Reference Design for Residential Energy Gateway, http://mechatronics.berkeley.edu/gateway.htm (last visited Mar. 9, 2009).

[55] *See* P.S. Subrahamanyam, David Wagner, Deirdre Mulligan, Erin Jones, Umesh Shankar, & Jack Lerner, CyberKnowledge & Univ. of Cal. at Berkeley, *Network Security Architecture for Demand Response/Sensor Networks* 87 (2006), *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/demand_response_CEC.pdf.

purposes the utility may need monthly totals of energy consumption; however it would not need to keep the intermediate granular measurements of consumption and load. Beyond the security advantages of reducing retention, shorter periods will likely yield benefits to regulable entities in terms of decreased storage and maintenance costs.[56] Monthly totals are less revealing and serve an important record-keeping purpose and can thus justifiably be retained for longer than near-real-time consumption information.

5. **Use Limitation:** Customer information should be used solely for the purposes specified in the notice. Sharing of such information should be only for a purpose compatible with the purpose for which it was collected.

Where regulable entities collect customer information for the primary purpose of providing energy service to the ratepayer, access to that data should be limited within the entity to departments with a justifiable requirement to use the data for fulfilling the clearly-specified purpose, such as the billing department. Any secondary uses beyond those must be specified in advance, and should only occur with explicit consumer consent under an affirmative consent regime, as introduced above.[57] For example, detailed information about a consumer's smart devices, such as a MAC address uniquely identifying the device and the manufacturer of the device, should not be used by a regulable entity or third party service provider, unless such use was specified to the consumer, who specifically and affirmatively consented to the use. Similarly, the entity should not share customer information or use it for behavioral advertising or other marketing purposes on behalf of a third party without explicit written authorization from the consumer. The Commission should require regulable entities to explain how they implement these use limitations.

6. **Data Quality and Integrity:** Regulable entities should, to the extent practicable, ensure that data is accurate, relevant, timely and complete. Regulable entities should provide consumers with tools to correct mistakes or challenge information provided in profiles.

Consumers need to be able to review and, where necessary, correct their information. This is required by section 8360(h), which states that customers must be provided information

[56] Robert Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete* (2002), http://epic.org/reports/dmfprivacy.html.
[57] *See supra* § V.A.2

and control options.[58] To comply with this requirement, the Commission should require regulable entities implement standards and technical requirements that will allow for easily-accessible interfaces that give consumers the opportunity to review and correct their customer information. Such review provides the best means of ensuring that consumer data is accurate.

7. **Data Security:** Regulable entities must protect customer information through appropriate security safeguards against risks of loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure, and Smart Grid technologies and services must be capable of implementing these security safeguards.

Reasonable security in the Smart Grid requires that any transmission of customer information must be secure and that regulable entities' data practices include meaningful safeguards for customer information. For example, encryption should be required for all communications that are sent over open wireless protocols or that could otherwise reasonably be intercepted on organization-owned infrastructure and third-party communication services. More broadly, the Commission should review technical standards for implementation and, if necessary, revise them to require that smart device communications provided by regulable entities be truly secure.

Further, customer information collected, used and maintained by regulable entities must be stored securely, made available only to those with a documented and authorized need for the information, and must be maintained subject to secure data management practices. If a security or other breach results in the loss or exposure of customer information, the regulable entity should be required to notify affected customers and take all reasonable steps to minimize harm to customers.

8. **Accountability and Auditing:** Regulable entities should be accountable for complying with these principles, should provide appropriate training to all employees and contractors who use customer information and should audit the actual use of that information to demonstrate compliance with the principles and all applicable privacy protection requirements.

The Commission should require regulable entities to have regular privacy training and ongoing awareness activities. Systems storing customer information should have access logs to document who is accessing private data. The Commission should require regulable entities to

[58] *See* Cal. Pub. Util. Code § 8360(h).

conduct regular audits of these logs to ensure that access is in compliance with appropriate and disclosed uses of the data. The Commission should further require rigorous reporting and auditing requirements that examine regulable entities' compliance and adoption of each of these privacy principles. Without a robust accountability and auditing mechanism, there will be no way for the Commission to ensure compliance with the various privacy commitments utilities make in their Smart Grid deployment plans.

B. The Principle of "Data Ownership" Alone Will Not Create Sufficient Privacy Protections for Consumers and Must Be Supplemented with the Fair Information Practice Principles

Consumer data ownership rules are often discussed as potential solution to privacy concerns. Although we generally support consumer ownership of data (assigning data ownership to utilities would turn them into information gatekeepers and could impede realization of both privacy and innovation policy goals), consumer ownership, alone, rarely solves privacy and security issues. Data ownership without attendant and real control over data can leave consumers with the limited ability to choose between alienating their data or not. Utilities and other third parties may require consumers to surrender control, if not ownership of customer information as part of service agreements and conditions of service. Instead, consumers need ongoing rights in their data—regardless of where it is stored and by whom it is held—complimented by assurances that those to whom they entrust it are bound by clear rules requiring them to abide by consumers' decisions. Such a framework respects the ongoing implications such data has for the consumer's privacy and safety.

The FIPs provide this broader privacy framework. FIPs do not require a specific data ownership regime, but are compatible with and complimentary to consumer data ownership. In particular the Transparency and Purpose Specification principles, discussed above in this section, ensure the data owner can make informed decisions about authorizing uses of data. The requirements of Data Quality and Integrity help the consumer maintain control over his data even when it is held by another party.

We encourage the Commission to recognize a consumer's ownership interest in customer information. However, to provide meaningful protections, the Commission needs to issue regulations that give consumers real control over their data even when it is held by third parties. The Fair Information Practice principles should provide the framework for the protections

necessary to ensure that utilities cannot force or induce consumers to contract away all their rights in their data, depriving them of any privacy protections.

C. Security and Privacy Principles Adopted by the Commission Should Specifically Require Data Breach Notification

Data breach notification is an important privacy practice implicated by the FIPs Data Security Principle. It warrants further elaboration and special attention by the Commission. California's Data Breach Notification Law, section 1789.29 of the Civil Code, made California a leader in data breach notification by requiring entities to report any breach in security to a system that contains personally identifiable information to all impacted individuals.[59] Forty-four other states have followed California's lead in this matter.[60]

We urge the Commission to keep California in the forefront of data breach notification by applying the requirements of section 1789.29 to regulable entities as part of their Smart Grid proposals. They should be required to report any breach of security in customer information to all impacted consumers and to the Commission.

Data breach notification rules will provide additional incentives for regulable entities to develop strong privacy and security standards. The cost and embarrassment resulting from breach notification can be a strong motivator. Further, by providing consumers' notice of data breaches, they can take appropriate measures to protect themselves from identity theft and other possible crimes. These notifications can also help the public and the Commission to evaluate regulable entities' security efforts.

VI. To Fulfill the Requirements of Senate Bill 17, the Commission Should Require Utilities to Employ Fair Information Practice Principles as Part of Utility Smart Grid Deployment Plans

The Commission has been tasked with determining the requirements for a Smart Grid deployment plan, which will guide the utilities in the development of their individual deployment plans.[61] It has asked for comments on the topics that should be addressed by the utilities'

[59] Cal. Civ. Code §§ 1798.29, 1798.82.
[60] Perkins Coie, *Security Breach Notification Chart* 134-35 (2008), *available at* http://www.digestiblelaw.com/files/upload/securitybreach.pdf (listing the effective dates for all forty-five states, plus Puerto Rico, that have enacted data breach notification laws).
[61] Feb. Joint Ruling, *supra* note 39, at 3.

plans.[62] It has also sought comment upon the proper evaluation and use of those deployment plans by the Commission.[63] We address both of these questions here.

In section V above, we have urged the Commission to adopt FIPs as a framework for ensuring privacy protections on the Smart Grid. Here, we specifically urge the Commission to incorporate the FIPs as requirements within the Smart Grid deployment plans. Specifically, utilities' deployment plans should take into account each of the following: (1) Transparency; (2) Individual Participation; (3) Purpose Specification; (4) Data Minimization; (5) Use Limitation; (6) Data Quality and Integrity; (7) Security; and (8) Accountability and Auditing.[64]

The Commission should ensure the privacy of the Smart Grid by requiring utilities to use the FIPs as part of their deployment plans in the following four ways. First, based on the FIPs, the Commission should define baseline privacy standards for Smart Grid deployment. Second, the Commission should require each utility to perform a privacy impact assessment as part of its Smart Grid planning process. Third, based on the assessment, each utility should adopt privacy practices meeting the minimum standards set by the Commission. These privacy practices should be responsive to each of the FIPs principles. Finally, the privacy impact assessments and the resulting privacy policies within the utilities' deployment plans should be revisited and re-approved in subsequent ratemakings and each time the Commission approves further investment pertaining to Smart Grid and Smart Device deployment. Only by an iterative process of problem definition, analysis, adoption, and review can the Commission and Californians be assured that their private information is being protected.

As part of the privacy impact assessment required by FIPs, a utility—in advance of actually building and deploying a system—would be required to answer key questions posed by the FIPs: What data will the utility be collecting? For what purpose? With whom will it share the data? How long will it keep the data? What confidence does it have that the data will be accurate and reliable enough for the purposes for which it will be used? How will it protect the data against loss or misuse? How will individuals have access to data about themselves? What audit, oversight and enforcement mechanisms will it have in place to ensure that it is following its own rules? The answers to these questions will provide important insights in the privacy and

[62] *Id.*
[63] *Id.* at 5-8.
[64] For a detailed discussion of these principles, please see *supra* § V.

security issues created by the Smart Grid. By identifying them early utilities can mitigate and guard against risks and protect consumer privacy at the lowest possible cost.

A. The Commission Should Require Regular Review of Privacy Impact Assessments and the Resulting Privacy Policies Contained in Deployment Plans

To ensure compliance with the deployment plan requirements described above, the Commission should require periodic reviews of privacy impact assessments and privacy policies. Utilities should be required to evaluate their implementation and success of their privacy policies and report their findings to the Commission. Further, the Commission should require appropriate revisions to the privacy impact assessments and privacy policies when deployment plans are modified. Similarly, new assessments and policies should be completed prior to any new deployment or revision to Smart Grid architecture. Any privacy lapses or data breaches should be evaluated by the Commission prior to awarding new rates or approving new deployments to determine if the utility is taking and has taken appropriate steps to remedy the problem and generally to protect privacy.

B. Privacy Considerations Must Be Built into the Design of the Smart Grid

Deployment plans can provide utilities an opportunity to address privacy concerns at an early design stage. Requiring strong privacy protections from the design stage will enable California's Smart Grid to maximize privacy and utility, while minimizing the cost of the protections. The Commission should require utilities adopt a "privacy by design" approach,[65] and build standards that reflect privacy interests into their deployment plans, rather than attempting to tack on privacy at a later point. Privacy by design is an effective and economically efficient means of protecting consumer privacy and security. Embedding privacy protections into the technology and design now, before smart meters and other Smart Grid technologies are fully deployed, and before the telecommunications infrastructures are installed, will prove 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.

[65] *See* Ann Cavoukian, Info. & Privacy Comm'r of Ont., *Privacy by Design*, http://www.privacybydesign.ca/ (last visited Mar. 9, 2010).

VII. The Commission Should Consider and Adopt Our Recommended Modification to the Proposed Access Rule, as Provided in Appendix A

As the February 8, 2010 Joint Ruling notes, "[t]he Commission has adopted a policy to provide that some third parties can have access to [customer] data with the customer's permission."[66] The ruling goes on to express concern about a number of unintended and unauthorized uses of the data that the Smart Grid may effectuate. Third-party access to customer data may support third-party services that provide some of the benefits of the Smart Grid; at the same time, third-party access represents its greatest privacy threat. A utility, for example, is specifically subject to this Commission's rules and specific statutes that limit data use and disclosure.[67] A non-utility third party possessing the same data, on the other hand, may 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. We support the Commission's suggestion to require customer authorization before a utility provides customer data to any third party. However, given the highly personal nature of the data that would potentially be shared, the Commission should adopt a strong privacy standard in its Proposed Access Rule[68] and should condition access on requirements that follow the Fair Information Practice principles.

Some third parties seeking access to customer data are likely to have business models based upon offering the consumer a service, perhaps for free, and then commercializing and selling the data. For example, a third-party service given access to granular usage data could offer consumers a useful service that helps them understand and control their energy consumption but base its profits on analyzing and selling behavioral information of interest to advertisers. Electronics retailers would like to know what appliances are in the home so they

---

[66] Feb. Joint Ruling, *supra* note 39, at 34.

[67] *See, e.g.*, Cal. Pub. Util. 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); D.97-12-088, app. A, § IV.A, *available at* 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."); Pac. Gas & Elec., *Rule 22 - Direct Access Rules* § C.3.a (1997), *available at* http://www.pge.com/tariffs/tm2/pdf/ELEC_RULES_22.pdf (requiring a customer to give written authorization for a utility to disclose usage data to direct access service providers); S.D. Gas & Elec., *Rule 25 - Direct Access Rules* § C.3.a (1999), *available at* http://www.sdge.com/tm2/pdf/ELEC_ELEC-RULES_ERULE25.pdf (same); S. Cal. Edison, *Rule 22 - Direct Access Rules* § C.3.a (2001), *available at* http://www.sce.com/NR/sc3/tm2/pdf/Rule22.pdf (same).

[68] Feb. Joint Ruling, *supra* note 39, app. B.

can market upgrades and accessories. A health insurance company may be interested in the number of hours a customer spends in front of the television. A dating website might be interested knowing that the number of residents at the household had recently fallen from two to one.

The consequences of utilities transferring customer data to third parties are significant. First, every copy and transmission of the data increases the risk of security breaches. Second, third parties may use the data in inappropriate or undisclosed ways. Third, the third parties may transfer the data on to yet other parties. Without proper protections, the customer could lose all control of her data once she authorizes third-party access. Customer trust in the Smart Grid is essential to its successful deployment and full adoption. Third-party misuse of data could be enough to undermine that trust. Therefore, the Commission's third-party data access rule should require utilities that deal with third parties to take appropriate steps to ensure that the third parties receiving data will provide appropriate privacy and confidentiality protections.

To actively protect against unexpected uses and the resulting harms, the Commission should adopt a robust regulatory framework granting affirmative control to customers as it extends to data generated by their households. This regulatory framework should attempt to maximize customer control over data and privacy protection, while enabling the benefits of the Smart Grid.

To reconcile these twin objectives, we propose a number of general changes to the Proposed Access Rule, based upon the Fair Information Practice principles. First, utilities should be required to obtain customer authorization based upon the full and complete disclosure of the uses that third parties will make of the data prior to giving third parties access to that information. If consumers agree to allow third-party access to such intimate information, the customer should be on specific notice of all uses prior to giving authorization. Second, utilities should be prohibited from sharing customer data with third parties unless the third parties agree, as a condition of receiving the data, to abide by specific FIPs principles, including: the full and complete disclosure of all uses of customer data; required reauthorization for changes in use; data breach notification; and privacy audits. The Commission should control downstream use of the data by conditioning access to the data on certain privacy and security requirements, including requiring regulated entities to condition third-party access to customer data on those

third parties agreeing to meet the requirements. The full text of our proposed rule can be found in Appendix A.

A. Before a Utility May Transfer Data to a Third Party, the Third Party Must Disclose Uses to and Obtain Authorization from Customers

To protect consumers' privacy and security, the Commission should require utilities to include customer privacy protections in their contracts and dealings with third parties. First, to avoid unauthorized uses of a customer's data by a third party, third parties should disclose all of the intended uses of customer data before authorization. This disclosure will enable customers to make an informed decision and permit informed consent. Thus, our suggested modifications to the proposed Rule place certain disclosure requirements on third parties that contract with utilities for customer data. It requires third parties to disclose to the customer, prior to the customer's authorization to provide access to the third party: (1) "each specific use of the customer data," (2) "all other parties with whom the entity will share customer data," and (3) "a list of all of the data elements that will be transferred to the entity. . . ."[69] Clearly articulating the purpose of the data use, all parties that will use the data, and the exact data being shared, enables the consumer to make an informed choice before deciding to share data.

Further, the Proposed Rule currently requires utilities to provide authorized third parties with "advanced meter data, including meter data used to calculate charges for electric service, historical load data and any other proprietary customer information. . . ."[70] The default rule should not be full disclosure of all proprietary customer information. Our modified Rule provides that utilities only disclose information "that is necessary to accomplish the uses specifically disclosed to and authorized by the customer."[71] Utilities should review third parties' disclosed uses and should only provide the individual data fields necessary for those disclosed uses.

B. Utilities Should Enforce Third Party Contractual Obligations

Once the utility transfers data to a third party a new set of risks and concerns arise. As described above, customer data is likely to be of interest to a wide variety of parties, for a wide

[69] *See infra* app. A, § 1(a)(i) (Modified Proposed Access Rule).
[70] *Id.* app. A, § 1.
[71] *Id.* app. A, § 1(b).

variety of purposes. Without intervention by the Commission, a third party that obtains customer information could sell that information to other third parties or use it in ways that were not authorized by the customer. The Commission should use its regulatory authority to ensure that any customer information transferred from a utility to a third party is sufficiently protected by requiring third parties to be contractually bound by the utilities as part of the consideration for receipt of customer data.

1. Prohibition On Non-Disclosed Uses and Parties

The Commission should require that utilities include clauses in contracts with third parties that require those third parties, as a condition of receiving customer data, to only use that data only for the specific purposes disclosed to the customer. Similarly, third parties should "not disclose customer data to any entities other than those entities expressly disclosed to and authorized by the customer. . . ."[72] For example, a consumer should not receive unsolicited advertisements based upon energy usage data that her energy efficiency consultant sold to appliance marketers without her authorization. If a third party later wants to use customer data for other uses or provide it to other parties, it must obtain "specific re-authorization, in writing or via electronic signature" for those new uses or other parties.[73]

2. Privacy Impact Assessments

As part of the regular privacy impact audits and assessments we recommend the utilities conduct,[74] the Commission should require all entities in possession of customer data to conduct, and report to the Commission, "independent audit[s] of the security of customer data and entity compliance with its disclosed usage policy. . . ."[75] Such assessments are critical to understanding whether measures to protect privacy are successful or if they create cost without providing sufficient benefit, will guide entities in improving practices, and support the Accountability and Auditing principle.

[72] *Id.* app. A, § 1(a)(ii).
[73] *Id.* app. A, § 1(a)(iii).
[74] *See supra* § V.A.8 (Accountability and Auditing).
[75] *See infra* app. A, § 2.

3. Data Quality and Integrity

Customers should have the right to see what data an entity possesses about them and to correct any inaccuracies in that data. The requirement is an important component of the FIPs Data Quality and Integrity principle, discussed in more detail above.[76] Our modified rule would require that entities possessing customer data "provide a means for customers to view their customer data held by the entity, a means to correct data inaccuracies, and a procedure to correct inaccuracies within thirty (30) days' notice of the inaccuracies."[77]

4. Data Destruction

Based upon the FIPs Data Minimization principle,[78] our modified Rule would require entities in possession of customer information to "destroy customer data when it is no longer necessary for the uses disclosed to the customer. . . ."[79] Destroying unnecessary data significantly reduces the risk of unauthorized use and disclosure of customer information.

5. Data Breach Notification

In Section V.C, we urged the Commission to apply California's Data Breach Notification Law, section 1789.29 of the Civil Code, to regulated entities. The Commission should likewise require third parties that handle customer data to notify customers and the Commission of any unauthorized disclosure, use, or access of the customer data, so that the customer can take appropriate steps to protect herself and modify her behavior accordingly (for example, by ceasing to share information with the party that allowed the breach). Requiring third parties to provide notification will provide strong incentives for safe and secure information practices so they can avoid the cost and embarrassment of having to report a data breach. Section 3(c) of our proposed Rule thus requires any entity in possession of proprietary customer information to follow the section 1789.29 data breach notification rules.

[76] *See supra* § V.A.6 (Data Quality and Integrity).
[77] *Id.* app. A, § 3(a).
[78] *See supra* §V.A.4 (Data Minimization).
[79] *See infra* app. A, § 3(b).

C. Other Third Party Access Rules That the Commission Should Consider

1. Government Access to Customer Information

We urge the Commission to specify, within the Proposed Access Rule, when and how utilities should provide customer information to law enforcement officials and other government agencies. Under both California and Federal law, the home, as a retreat from the outside world and from the government, is an especially protected space, with an especially strong privacy interest attached to it.

Longstanding United States constitutional values and precedent afford special protection for activities occurring within the sanctity of individuals' homes because of their inherently personal nature. The Fourth Amendment draws "a firm line at the entrance to the house,"[80] because "privacy expectations are most heightened" in the "private home."[81] The Supreme Court affirmed this protection for all types of data found in the home, noting in *Kyllo v. United States* that the "Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained. . . . In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."[82] In *Kyllo*, the Court invalidated the warrantless use of thermal imaging technology to measure heat emanating from a home as an unlawful search under the Fourth Amendment, despite the lack of any physical intrusion into the home by law enforcement.[83] Data collected via Smart Grid technologies is similarly revealing of the intimate details of home life and should be subject to at least the same high levels of protection that the Supreme Court required of law enforcement in *Kyllo*.

Californian's constitutional privacy protections extend further than general Fourth Amendment protections and have been found to protect business records.[84] Although the California Supreme Court has not yet addressed energy privacy, it has recognized a protected privacy interest in other records held by third parties. For example, in *Burrows v. Superior*

---

[80] *Payton v. New York*, 445 U.S. 573, 590 (1980).
[81] *Dow Chemical Co. v. United States*, 476 U.S. 227, 237 n.4 (1986); *see Boyd v. United States*, 116 U.S. 616, 630 (1886) ("It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property[.]").
[82] *Kyllo v. United States*, 533 U.S. 27, 37 (2001).
[83] *Id*. at 40.
[84] *See, e.g.*, *Valley Bank of Nev. v. Superior Court*, 15 Cal. 3d 652 (1975).

Court,[85] the court held that customer information voluntarily disclosed by a bank to law enforcement officers without the customer's knowledge or consent was the product of an unlawful search and seizure under article I, section 13, of the California Constitution. The court went on to hold that customers expect that the information they share with their banks will remain private, and that "absent compulsion by legal process . . . [the customer expects the matters he] reveals to the bank will be utilized by the bank only for internal banking purposes."[86] Later cases have similarly protected telephone records.[87]

Article 1, section 1 of the California Constitution provides additional protections. In *Brillantes v. Superior Court*, the court held that "an intrusion upon constitutionally protected areas of privacy requires a balancing of the juxtaposed rights, and the finding of a compelling state interest."[88] The court allowed the seizure of medical records only where "the state [had] demonstrated a compelling interest in the medical records related to the Medi-Cal fraud investigation."[89] Similarly, in *McKirdy v. Superior Court*, the court affirmed "any [incursion into individual privacy] must be justified by a compelling interest."[90]

The Commission has already recognized that the privacy protections inherent in sections 1 and 13 of article 1 of the California Constitution extend to cover customer energy data. In Decision No. 90-12-121 and its appeal, Decision No. 01-07-032, the Commission extensively examined privacy concerns related to law enforcement access to utility data and, relying on the *Burrows*,[91] *Blair*,[92] and *Chapman*[93] line of cases, determined that it should not be disclosed to law enforcement without adequate legal process.[94] We urge the Commission to follow this precedent and re-affirm that law enforcement and government agencies must obtain adequate legal process before accessing customer energy usage data. Because of the unusually private nature of granular energy usage data, we urge the Commission to go a step further and require law enforcement to show probable cause in the form of a warrant before a utility releases such

[85] 13 Cal. 3d 238 (1974).
[86] *Id*.
[87] *People v. Blair*, 25 Cal. 3d 640, 653-54 (1979); *People v. Chapman*, 36 Cal. 3d 98 (1984).
[88] 51 Cal. App. 4th 323, 340 (1996).
[89] *Id.* at 342.
[90] 138 Cal. App. 3d 12, 22 (1996).
[91] 13 Cal. 3d 238.
[92] 25 Cal. 3d 640.
[93] 36 Cal. 3d 98.
[94] D.90-12-121; D.01-07-032.

data. Providing such data to law enforcement without a warrant would be inconsistent with Californians' constitutional right to privacy[95] and the federal Constitution.

2. Civil Litigant Access to Customer Information

In the context of civil litigation, given the sensitivity of smart meter data and its potential to reveal private details of home life, there should be a preference for seeking such data not from the utility, but from the customer directly (who, under our recommendations, should have access to data pertaining to his or her home energy usage). If the only way a civil litigant can obtain the information is directly from a regulable entity, then the litigant should be required to show a compelling interest in the information.

In *White v. Davis*,[96] the first California Supreme Court case to interpret article 1, section 1, of the state constitution, the Court solidified Californian's right to informational privacy. The court held that the constitutional privacy right protects citizens from use of personal information "for another purpose or the disclosure of it to some third party."[97] The court later held in *Hill v. National Collegiate Athletic Assn.,*[98] and affirmed in *American Academy of Pediatrics v. Lungren*,[99] that in cases where there is an obvious invasion of a right fundamental to informational privacy or autonomy, a "compelling interest must be present to overcome the vital privacy interest."[100] If, in contrast, the privacy interest is less central, or in bona fide dispute, a general balancing test is employed.[101] Because of the intrusive nature of energy usage data, as described above, civil litigants should be required to show a compelling interest in the information.

Further, California case law has held that entities receiving subpoenas for private information on their customers must notify the customers prior to disclosing the information and allow time for them to respond. The Commission should similarly protected customer energy information. In *Valley Bank of Nevada v. Superior Court,* the California Supreme Court held that "before confidential customer information may be disclosed in the course of civil discovery

---

[95] Cal. Const. art. I, §§ 1, 13.
[96] 13 Cal 3d 757 (1974).
[97] *Id*. at 775.
[98], *Hill v. Nat'l Collegiate Athletic Assn.,* 7 Cal. 4th 1 (1994).
[99] *Am. Academy of Pediatrics v. Lungren,* 16 Cal. 4th 307 (1997).
[100] *Hill*, 7 Cal. 4th at 34.
[101] *Id.*

proceedings, [a] bank must take reasonable steps to notify its customer."[102] Similarly, in *Sehlmeyer v. Department of General Services*, the court held that the constitutional right to privacy requires "that an administrative subpoena duces tecum [seeking a third party witness's medical records] must be preceded by notice to the witness."[103] The courts have also recognized the need to "afford the third party a fair opportunity to assert her interests by objecting to disclosure, by seeking an appropriate protective order[,] or by instituting other legal proceedings to limit the scope or nature of [discovery]."[104]

To keep utility practices in line with California case law, the Commission should require that utilities and other regulated entities only disclose customer data to civil litigants upon being provided with a court order based on a showing of compelling interest and after notifying the customer to provide her with a chance to object.

3. Rules Regarding Third-Party Handling of Customer Information Received Directly from Consumers

The discussion above urges the Commission to adopt rules regulating the use of customer information by utilities and third parties to whom utilities provide customer data. These suggestions are in response to the Commission's specific questions regarding these entities. However, numerous other third parties presently obtain, or plan to obtain, energy usage data directly from the consumer via devices installed in the home, below the meter. For example, Google's' "Power Meter" device captures energy usage data directly from consumers, below the meter. Google presently does not charge for the service.[105] In these situations, the utilities may not be able to act as a gatekeeper for the information. The customer data obtained by these third parties is no less private than the customer data collected and transferred by the utilities, nor would its misuse be any less invasive. As such, we urge the Commission and other regulators to adopt rules similar to the ones outlined here[106] for all parties collecting, using, and transmitting customer information, whether they obtain that data above or below the meter.

---

[102] 15 Cal. 3d 652, 658 (1975).
[103] 17 Cal. App. 4th 1072, 1079 (1993).
[104] *Id.* at 1085 (citing *Valley Bank of Nev. v. Superior Court*, 15 Cal. 3d 652, 658 (1975)).
[105] For information on Google's service, see Google Power Meter, Frequently Asked Questions, http://www.google.org/powermeter/faqs.html (last visited Mar. 9, 2010).
[106] *See supra* §§ VII.A, B; *see also infra*, app. A.

VIII. The Commission Should Include Privacy-Related Quantitative Metrics for Smart Grid Implementations

We support the Commission's proposed use of metrics as a measure of Smart Grid deployment and strongly support the specific use of privacy metrics as a means of measuring the privacy vulnerabilities of the deployed Smart Grid. We recommend that such metrics should be required components of all Smart Grid deployment plans and should be updated by regulated utilities in subsequent proceedings relating to discrete Smart Grid implementations and ratemakings. We propose the following additions and modifications to the Commission's proposed metrics in Attachment C of the Joint Ruling, based on our identification of privacy risks in Section II.B and discussion of Fair Information Practice principles in Section V above.

A. Cyber Security Metrics

The Commission should add the following metrics to Section 2 of the Proposed Metrics to fill the placeholder for cyber security metrics:

- Number of security breaches experienced by the utility or third parties to which the utility provides customer information.
- Number and percentage of customers affected by the security breaches.
- Number and percentage of customer records accessed during the security breaches.
- Average number of days between the security breach and when the customers are notified.
- Number of attempted cyber attacks on the utility or third parties to which the utility provides customer information.
- Monetary damages suffered by utilities or consumers as a result of cyber attacks on the utility or its infrastructure.
- Amount of annual operational expenditure on cyber security.
- Percentage of expenditure on cyber security in the overall operating expense.

- Amount of damages incurred to customers' smart devices as a result of cyber attacks.

- Number of security and privacy impact assessments performed by utilities.

B. Privacy Metrics

We also recommend the following modifications and additions to the proposed metrics in Attachment C of the Joint Ruling to prevent additional privacy harms and to give the Commission specific insight into consumer privacy protections:

- Remove the first item under Section 5 which presently reads "the number and percentage of electricity customers . . . served by appliances and/or equipment which can communicate information automatically about on/off status and availability for load control." This proposed metric encourages the use of customer devices to reveal detailed status information to the utility. This metric is adverse to the privacy interest of residential customers and should be removed.

- Allowing customers to control the granularity of data flowing outside their homes is crucial to privacy. Therefore, we recommend adding the following metrics to Section 9 "Provide Consumers with Timely Information and Control Options:"
    - Number of customers able to control the time interval of smart meter reading reported to utility.
    - Number of customers that exercise control over the time interval of smart meter reading reported to utility.
    - Number of customers able to control their smart devices with their own Energy Management System.
    - Number of customers that exercise control over their smart devices with their own Energy Management System.

- Customer concern about privacy represents a barrier to Smart Grid adoption. Therefore, we recommend adding the following metrics to Section 11 "Lowering Barriers to Adoption of Smart Grid:"
    - Amount of customer information collected about an average residential customer and retention period of such data.
    - Number and type of third party entities receiving customer information under the [Proposed] Access Rule.
    - Number and type of law enforcement or other government requests to access customer information held by the utility or the third parties to whom the utility provides information, and the compliance with such requests.
    - Number of individuals whose customer information was provided to law enforcement or other government agencies.
    - Number and type requests by civil litigants to access customer information held by the utility and the compliance with such requests.
    - Number and type of third parties to whom the utility provides information, and the compliance with such requests.
    - Number and type of data breach notifications during the reporting period.

Finally, the Commission should delete the first metric in Section 6 of the Proposed Metrics: "Number of consumer devices actively communicating with Home Area Networks." This metric is detrimental to data minimization and therefore to privacy protection, as it requires utilities to obtain information about appliances within consumers' homes. A consumer may have deployed a Home Area Network for the express purpose of protecting her privacy by hiding the devices within the home from the utility. Such metrics, relating to in-home deployment, should take into account the fact that privacy-friendly smart devices may be invisible to the utilities. The Commission's metrics should respect customers' desire for privacy and not encourage the utilities to collect detailed device information from residential customers.

IX. The Commission Should Not Wait for Privacy Standards from the National Standard-Setting Bodies, and Should Adopt Fair Information Practice Principles Now

State Senate Bill 17 instructs the Commission to "adopt standards and protocols to ensure functionality and interoperability developed by public and private entities, including, but not limited to, the National Institute of Standards and Technology, Gridwise Architecture Council, the International Electrical and Electronics Engineers, and the National Electric Reliability Organization recognized by the Federal Energy Regulatory Commission."[107] As the Commission has observed, however, the national standard-setting organizations have not yet released final drafts of their standards and protocols.[108] The Commission seeks comment on three possible approaches to this problem.

1) Deferring Commission consideration in this proceeding until a number of the listed agencies have adopted standards or protocols;

2) Deferring Commission consideration of protocols to another proceeding that will commence after a number of the listed agencies have adopted standards or protocols; or

3) Adopting a "performance standard" in this proceeding requiring that those implementing a Smart Grid technology take steps to ensure that it has the capability to function and operate with devices developed pursuant to standards adopted by major standard setting agencies.[109]

In light of the rapid deployment of Smart Grid technologies already underway in California, approaches (1) and (2) above appear as problematically slow for addressing adequately issues of privacy and consumer protection. It is unclear how long it will take for "a number of the listed agencies" to adopt standards; smart devices deployed during this open-ended time period, risk non-compliance with both the technical standards and privacy standards that the Commission eventually adopts.

At the same time, approach (3) appears not to address privacy issues, at all, as the

[107] Cal. Pub. Util. Code § 8362.
[108] Feb. Joint Ruling, *supra* note 39, at 19.
[109] *See id*. These three options are slightly reworded from the language in the original ruling.

"functional operability with other devices" requirement carries no privacy protections or restrictions. Further, approach (3) shifts significant standards decision-making authority to the utilities themselves, creating a self-regulatory regime and depriving the utilities of meaningful Commission guidance on relevant standards. For this reason, it is unclear whether approach 3 succeeds in meeting the obligations imposed by SB 17.

We thus urge the Commission to pursue a fourth option, at least with regard to privacy requirements. The Commission should adopt concrete privacy requirements based on the Fair Information Practice principles without delay, and should compare technical and other standards presented to it against these requirements. If national standards or guidelines related to privacy protections are promulgated in the future, the Commission can open a new proceeding to consider these.

As described further above in Section V,[110] the FIPs are a widely recognized and well established framework for information management. Indeed, it is unlikely that any of the national standard-setting organizations would release privacy standards that were not reflective of, or influenced by, the Fair Information Practice principles. If the Commission later considers adoption of standards from these national standard-setting organizations, we urge the Commission to disregard outright any set of standards that does not reflect the FIPs framework.

Privacy is a valued constitutional right in California, and the Commission has adequate authority, under article 1, section 1 of the California Constitution to adopt Smart Grid privacy standards immediately and on its own initiative,[111] independent of authority granted it by SB 17. We urge that the Commission adopt the Fair Information Practice principles as California's Smart Grid privacy protection framework. California also has a strong history of being at the forefront of both environmental and privacy regulation. Where California leads, the rest of the states and the federal government follow. The Smart Grid provides the Commission with an opportunity to help California to continue to lead the country in environmental regulation and privacy protection.

[110] For a comprehensive overview and explanation of the FIPs, please refer to § V, *supra*.
[111] *See* discussion *supra* § III.

X. Conclusion

The Center for Democracy & Technology and the Electronic Frontier Foundation appreciate the opportunity to submit these comments in response to the Assigned Commissioner and Administrative Law Judge's Joint Ruling Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid, issued February 8, 2010. We commend the Commission on its careful consideration of the consumer privacy risks presented by the emerging Smart Grid, and we thank the Commission again for its consideration of the privacy recommendations we have presented here.

Respectfully submitted this March 9, 2010 at San Francisco, California.

/s/ Jennifer Lynch

JENNIFER LYNCH, Attorney
Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7515
Attorney for CENTER FOR DEMOCRACY & TECHNOLOGY

/s/ Lee Tien

LEE TIEN, Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333 x102
Attorney for ELECTRONIC FRONTIER FOUNDATION

APPENDIX A – Modifications to Language of Proposed Third Party Access Rules[112]

1. An electrical corporation shall provide a customer, the customer's electric service provider (ESP), the customer's demand response provider (DRP), or other third party entity authorized by the customer read-only access to the customer's advanced meter data, including meter data used to calculate charges for electric service, historical load data and any other proprietary customer information (collectively, "customer data") only as described herein in sections 1 through 8. ESPs, DRPs, or any other third parties that obtain customer data shall not disclose or use that customer data except as described herein in sections 1 through 8. The access shall be convenient and secure, and the data shall be made available no later than the next day of service. Such authorization may be made in writing or via electronic signature, consistent with industry, privacy and security standards and methods. The utility may only transfer customer data:

    a. to an entity that is either (i) already bound by this section or (ii) contractually agrees, in consideration of receiving the data, to

        i. fully disclose to the customer, prior to obtaining authorization:

            1. each specific use of the customer data,

            2. all other parties with whom the entity will share the customer data, and

            3. a list of all of the data elements that will be transferred to the entity (these may include, for example, name, address, social security number, meter readings [including the frequency of measurements being provided], appliance ID numbers, or any other discrete types of information being transferred);

[112] Throughout this Appendix A, we have used specific formatting to denote changes. The proposed additions that the Commission denoted in its Feb. Joint Ruling with underlined text have been included in our Appendix text without an underline. We have illustrated our further additions with an underline. Text that is formatted with a strikethrough *only* represents the text in the Feb. Joint Ruling that was also presented in strikethrough. Text that is contains both an *underline and a strikethrough* is text that was provided in the Feb. Joint Ruling and that we recommend omitting.

ii. not disclose customer data to any entities other than those entities expressly disclosed to and authorized by the customer under (i), above;

iii. obtain separate, specific re-authorization, in writing or via electronic signature, for any new use of customer data or new entity with which it plans to share the data, consistent with (i), above; and

iv. abide by the regulations in sections 2 and 3, below; and

b. that is necessary to accomplish the uses specifically disclosed to and authorized by the customer.

2. An electrical corporation or other entity providing customer data shall use at a minimum industry standards and methods for providing secure customer, ESP, DRP and third party access to a specified customer's ~~meter~~ data. For purposes of these Rules, "industry standards" shall include those industries that routinely deal with highly personal, sensitive and confidential information, including but not limited to the financial industry and the medical information industry. ~~[The electrical corporation~~ All entities in possession of customer data shall have an independent security audit of the mechanism for customer and third party access to ~~meter~~ customer data conducted within one year of initiating such access and report the findings to the Commission.~~]~~ Thereafter, all entities in possession of customer data shall have an independent audit of the security of customer data and entity compliance with its disclosed usage policy on an annual basis and shall report the findings to the Commission, which shall make the reports publicly available.

3. All entities in possession of customer data shall:

a. provide a means for customers to view their customer data held by the entity, a means to correct data inaccuracies, and a procedure to correct inaccuracies within thirty (30) days' notice of the inaccuracies;

b. destroy customer data when it is no longer necessary for the uses disclosed to the customer;

c. follow the data breach notification rules described in Cal. Civ. Code § 1798.29, for the loss or unauthorized acquisition of or access to customer data; and,

d. only disclose customer data to law enforcement after being provided with a warrant.

e. only disclose customer data to civil litigants after being provided with a court order based on a showing of compelling interest and after notifying the customer to provide the customer with a chance to object to disclosure.

4. ~~3.~~ The California Independent System Operator, or any subsequent regional transmission organization or regional reliability entity, shall have access only to information necessary or required for wholesale settlement, load profiling, load research and reliability purposes.

5. ~~4.~~ A customer may authorize, either in writing or by electronic signature, its customer data to be available to an entity other than its Load Serving Entity or Utility Distribution Company, subject to the requirements of sections 1 through 3.

6. ~~5.~~ An electrical corporation shall provide access to data, as described above, in a manner consistent with and in accordance with the time frame as decided by the Commission in Decision _____,

   Revised rule modeled on Tariff Rule 22[56]

7. ~~3.~~ Providing Access to Customer Data Captured by AMI for Authorized Third Parties

   [Insert utility] will only provide customer-specific usage data to parties specified and authorized by the customer, subject to the provisions in sections 1 through 3 above, and the following provisions:

   a. ~~Except as provided in Section d, t~~The inquiring party must have ~~written~~ authorization from the customer, either in writing or by electronic signature, to release such

[56] Tariff Rule 22 was the tariff adopted by electric utilities to provide for Direct Access Service. A copy of PG&E's Tariff Rule 22 is available online at: external link: http://beta1.pge.com/nots/rates/tariffs/pdf/ER22.pdf. The relevant portion is at C.3, on tariff sheets 11-12.

information to the inquiring party only. Such authorization must be revocable. At the customer's request, this authorization may also indicate if customer information may be released to other parties as ~~specified~~ specified and authorized by the customer.

b. Subject to customer authorization, [~~I~~insert utility] will provide ~~a maximum of~~ not more than the most recent twelve (12) months of customer usage data ~~or the amount of data for that specific service account~~ in a format consistent with industry standards, including privacy and security standards, as approved by the Commission. Customer information will be released to the customer or an authorized agent ~~up to two (2) times per year per service account~~ at no cost to the ~~requesting party~~ or the customer. ~~Thereafter, [insert utility] will have the ability to assess a processing charge only if approved by the Commission.~~

c. ~~As a one time requirement at the initiation of Direct Access, [~~i~~~~I~~nsert utility] will make available a database containing a twelve (12) month history of customer-specific customer's data usage information with geographic and SIC information, but with customer identities removed, to a ~~customer's ESP, DRP or other~~ third party~~ies~~ approved by the Commission, subject to the requirements of this provision and provisions 1 through 3, and only where a customer has authorized such disclosure. ~~[Insert utility] will have the ability to assess a charge only if approved by the Commission.~~

~~d. By electing to take Direct Access service from an ESP, the customer consents to release to the ESP metering information required for billing, settlement and other functions required for the ESP to meet its requirements and twelve (12) months of historical data.~~

d. A third party receiving customer data pursuant to this section shall use such data only for the purposes to which the consumer consented and shall be subject to the same rules on privacy and security that are applicable to utilities handling customer data.

~~d. By authorizing third party to access their information, the customer consents to release to a third party information required for billing, settlement and other functions~~

and services required for that entity to meet its requirements and obligations and twelve (12) months of historical data.

CERTIFICATE OF SERVICE

I hereby certify that, pursuant to the Commission's Rules of Practice and Procedure, I have this day served a true copy of this document, JOINT COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY AND THE ELECTRONIC FRONTIER FOUNDATION ON PROPOSED POLICIES AND FINDINGS PERTAINING TO THE SMART GRID, on all parties identified on the attached official service list for Proceeding: R08-12-009. Service was completed by serving an electronic copy on their email address of record and by mailing paper copies to parties without email addresses.

Executed on March 9, 2010 at Berkeley, California

/s/ Jennifer Lynch
JENNIFER LYNCH, Attorney
Samuelson Law, Technology & Public Policy Clinic
University of California – Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200

SERVICE LIST

carlgustin@groundedpower.com
jeffrcam@cisco.com
cbrooks@tendrilinc.com
npedersen@hanmor.com
slins@ci.glendale.ca.us
douglass@energyattorney.com
ffletcher@ci.burbank.ca.us
kris.vyas@sce.com
atrial@sempra.com
lburdick@higgslaw.com
liddell@energyattorney.com
mshames@ucan.org
ctoca@utility-savings.com
bobsmithttl@gmail.com
mtierney-lloyd@enernoc.com
ed@megawattsf.com
mterrell@google.com
mdjoseph@adamsbroadwell.com
pickering@energyhub.net
margarita.gutierrez@sfgov.org
lms@cpuc.ca.gov
fsmith@sfwater.org
srovetti@sfwater.org
tburke@sfwater.org
lettenson@nrdc.org
marcel@turn.org
mkurtovich@chevron.com
SSchedler@foe.org
cjw5@pge.com
nes@a-klaw.com
pcasciato@sbcglobal.net
steven@sfpower.org
mgo@goodinmacbride.com
mday@goodinmacbride.com
ssmyers@worldnet.att.net
lex@consumercal.org
farrokh.albuyeh@oati.net
Service@spurr.org
wbooth@booth-law.com
jwiedman@keyesandfox.com
kfox@keyesandfox.com
enriqueg@greenlining.org
gmorris@emf.net
kerry.hattevik@nrgenergy.com
rquattrini@energyconnectinc.com
seboyd@tid.org
martinhomec@gmail.com
dzlotlow@caiso.com
dennis@ddecuir.com
scott.tomashefsky@ncpa.com
jhawley@technet.org
lnavarro@edf.org
Lesla@calcable.org
cbk@eslawfirm.com
gstaples@mendotagroup.net
jlin@strategen.com
MNelson@MccarthyLaw.com
EGrizard@deweysquare.com
Mike.Ahmadi@Granitekey.com
r.raushenbush@comcast.net
tam.hunt@gmail.com
john.quealy@canaccordadams.com
mark.sigal@canaccordadams.com
barbalex@ctel.net
crjohnson@lge.com
julien.dumoulin-smith@ubs.com
david.rubin@troutmansanders.com
jennsanf@cisco.com
marybrow@cisco.com
jmccarthy@ctia.org
jay.birnbaum@currentgroup.com
bboyd@aclaratech.com
bob.rowe@northwestern.com
monica.merino@comed.com
sthiel@us.ibm.com
ed.may@itron.com
rgifford@wbklaw.com
leilani.johnson@ladwp.com
dschneider@lumesource.com
david@nemtzow.com
cjuennen@ci.glendale.us
fhall@solarelectricsolutions.com
mark.s.martinez@sce.com
case.admin@sce.com
michael.backstrom@sce.com
nquan@gswater.com
Jcox@fce.com
esther.northrup@cox.com

kfoley@sempra.com
kmkiener@cox.net
ygross@sempra.com
rwinthrop@pilotpowergroup.com
CentralFiles@semprautilities.com
tcahill@semprautilities.com
cmanson@semprautilities.com
jerry@enernex.com
traceydrabant@bves.com
peter.pearson@bves.com
dkolk@compenergy.com
ek@a-klaw.com
rboland@e-radioinc.com
sue.mara@rtoadvisors.com
juan.otero@trilliantinc.com
mozhi.habibi@ventyx.com
faramarz@ieee.org
elaine.duncan@verizon.com
mandywallace@gmail.com
norman.furuta@navy.mil
kgrenfell@nrdc.org
mcarboy@signalhill.com
nsuetake@turn.org
bfinkelstein@turn.org
andrew_meiman@newcomb.cc
ayl5@pge.com
DNG6@pge.com
fsc2@pge.com
filings@a-klaw.com
Kcj5@pge.com
mpa@a-klaw.com
rcounihan@enernoc.com
stephen.j.callahan@us.ibm.com
tmfry@nexant.com
bcragg@goodinmacbride.com
bdille@jmpsecurities.com
cassandra.sweet@dowjones.com
jscancarelli@crowell.com
jas@cpdb.com
nml@cpdb.com
SDHilton@stoel.com
Diane.Fellman@nrgenergy.com
cem@newsdata.com
lisa_weinzimer@platts.com
prp1@pge.com
achuang@epri.com
caryn.lai@bingham.com
epetrill@epri.com
ali.ipakchi@oati.com
chris@emeter.com
sharon@emeter.com
ralf1241a@cs.com
sean.beatty@mirant.com
john_gutierrez@cable.comcast.com
t_lewis@pacbell.net
Valerie.Richardson@us.kema.com
nellie.tong@us.kema.com
Douglas.Garrett@cox.com
rstuart@brightsourceenergy.com
mrw@mrwassoc.com
cpucdockets@keyesandfox.com
dmarcus2@sbcglobal.net
rschmidt@bartlewells.com
jlynch@law.berkeley.edu
jurban@law.berkeley.edu
kco@kingstoncole.com
philm@scdenergy.com
j_peterson@ourhomespaces.com
joe.weiss@realtimeacs.com
michaelboyd@sbcglobal.net
bmcc@mccarthylaw.com
sberlin@mccarthylaw.com
mary.tucker@sanjoseca.gov
tomk@mid.org
joyw@mid.org
brbarkovich@earthlink.net
gayatri@jbsenergy.com
dgrandy@caonsitegen.com
demorse@omsoft.com
martinhomec@gmail.com
e-recipient@caiso.com
hsanders@caiso.com
jgoodin@caiso.com
wamer@kirkwood.com
tpomales@arb.ca.gov
brian.theaker@dynegy.com
danielle@ceert.org
dave@ppallc.com
jmcfarland@treasurer.ca.gov
shears@ceert.org
kellie.smith@sen.ca.gov
lkelly@energy.state.ca.us

mgarcia@arb.ca.gov
ro@calcable.org
steven@lipmanconsulting.com
lmh@eslawfirm.com
abb@eslawfirm.com
bsb@eslawfirm.com
glw@eslawfirm.com
jparks@smud.org
ljimene@smud.org
ttutt@smud.org
vzavatt@smud.org
vwood@smud.org
dan.mooy@ventyx.com
kmills@cfbf.com
rogerl47@aol.com
jellis@resero.com
michael.jung@silverspringnet.com
wmc@a-klaw.com
bschuman@pacific-crest.com
sharon.noell@pgn.com
californiadockets@pacificorp.com
ag2@cpuc.ca.gov
agc@cpuc.ca.gov
am1@cpuc.ca.gov
crv@cpuc.ca.gov
df1@cpuc.ca.gov
dbp@cpuc.ca.gov
trh@cpuc.ca.gov
fxg@cpuc.ca.gov
gtd@cpuc.ca.gov
jw2@cpuc.ca.gov
jdr@cpuc.ca.gov
jmh@cpuc.ca.gov
kar@cpuc.ca.gov
kd1@cpuc.ca.gov
lau@cpuc.ca.gov
zaf@cpuc.ca.gov
mjd@cpuc.ca.gov
mc3@cpuc.ca.gov
wtr@cpuc.ca.gov
rhh@cpuc.ca.gov
srt@cpuc.ca.gov
scl@cpuc.ca.gov
scr@cpuc.ca.gov
tjs@cpuc.ca.gov
vjb@cpuc.ca.gov
wmp@cpuc.ca.gov
BLee@energy.state.ca.us
ab2@cpuc.ca.gov