BEFORE THE PUBLIC UTILITIES COMMISSION OF THE

STATE OF CALIFORNIA

FILED
10-15-10
04:59 PM

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)

PROPOSED SMART GRID PRIVACY POLICIES AND PROCEDURES—
OPENING RESPONSE OF
THE CENTER FOR DEMOCRACY & TECHNOLOGY
AND THE ELECTRONIC FRONTIER FOUNDATION
TO ASSIGNED COMMISSIONER'S RULING OF SEPTEMBER 27, 2010

JENNIFER URBAN, Attorney[1]
Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley School of Law
585 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7338
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: October 15, 2010

[1] Berkeley Law students Heather Patterson and Evan White 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)

PROPOSED SMART GRID PRIVACY POLICIES AND PROCEDURES—
OPENING RESPONSE OF
THE CENTER FOR DEMOCRACY & TECHNOLOGY
AND THE ELECTRONIC FRONTIER FOUNDATION
TO ASSIGNED COMMISSIONER'S RULING OF SEPTEMBER 27, 2010

I. Introduction

The Center for Democracy & Technology ("CDT")[2] and the Electronic Frontier Foundation ("EFF")[3] jointly file these comments in response to the Assigned Commissioner's Ruling of September 27, 2010 ("Ruling") requesting proposals setting forth "policies and procedures that will help protect the privacy of a customer's data, will help ensure its security and will permit access to the information by authorized third parties."[4]

Both the Commission[5] and parties to this proceeding[6] have affirmed that the best available framework for developing privacy and security rules for household energy usage data

[2] CDT 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.

[3] 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.

[4] Assigned Commissioner's Ruling of September 27, 2010 at 6.

[5] D.10-06-047 at 41-42.

[6] *E.g.*, Prehearing Conference Statement of Pacific Gas and Electric Company (U 39 E) on Privacy and Security Policies at 2; Prehearing Conference Statement of San Diego Gas & Electric Company's (U 902-E) and Southern California Gas Company (U 904 G) at 8-9; Prehearing Conference Statement of Southern California Edison Company (U 338-E) at 6.

is the full set of "Fair Information Practice" principles, as previously outlined by CDT and EFF.[7] Adopting rules based on the full set of FIPs is particularly important now, in light of a growing national consensus that consumer privacy is not adequately protected by mere "notice and choice."[8] In the context of the Smart Grid, a notice-and-choice-based approach could leave customers uninformed about the many ways in which their household energy data is being collected and used. Notice-and-choice also fails to address other important issues, such as accuracy and security. Therefore, the Commission has appropriately recognized the full set of FIPs.[9]

In the Appendix to this comment, we articulate a clear, concise set of policies and procedures that implement or "operationalize" the full set of FIPs for the Smart Grid. We respectfully encourage the Commission to require these policies and procedures of all regulable Smart Grid entities. CDT and EFF are interested in working with all parties on these proposed rules, and we invite other parties to offer suggestions for improvement or to express support for our framework. We look forward to reviewing the factual information and the policies and procedures submitted by the utilities and third parties in response to the Ruling,[10] in order to understand more completely how data will flow in the Smart Grid, and how utilities and third parties plan to protect customer privacy while collecting, using, and sharing household energy usage data. However, we believe that our proposed rules constitute a reasonable, balanced and effective approach to privacy that will work across a variety of business models.

In drafting these proposed rules, we had in mind three different relationships or data flows that might develop for home energy usage information:

---

[7] See, e.g., Joint Comments of CDT and EFF (March 9, 2010) available at http://www.cdt.org/files/pdfs/20100309_smartgrid_cpuc_comments.pdf; Comments of Privacy and Cyber Security Law and Policy Researchers (March 9, 2010) http://docs.cpuc.ca.gov/efile/CM/114759.pdf; Comments of Tendril, Appendix A, p.2 (March 9, 2010) http://docs.cpuc.ca.gov/efile/CM/114794.pdf ("[I]t is recognized that the detailed information required for and generated by the many smart grid technologies and applications will allow far more raw and granular data regarding individual and aggregate energy usage across populations. Such a change raises obvious and non-trivial privacy concerns that we discuss in more detail in these comments.").

[8] Steve Lohr, Redrawing the Route to Online Privacy, N.Y. Times, Feb. 27, 2010, at BU4 ("'There are essentially no defenders anymore of the pure notice-and-choice model,' said Daniel J. Weitzner, a senior policy official at the National Telecommunications and Information Administration of the Commerce Department. 'It's no longer adequate.'").

[9] D.10-06-047 at 41-42.

[10] Ruling of September 27, 2010, sections 3.2-3.5, at 3-6.

- A third party under contract with a utility receives energy usage information from the utility and uses that information to provide services on behalf of the utility. Since the third party is a contractor of the utility, customer consent should not be required for the utility to disclose information to this third party initially, but the customer should receive notice of the practice, and the third party should be bound by all the rules that would apply to the utility, including limits on secondary use and onward disclosure. For services not essential to the provision of electrical service, such as demand response, energy management, and energy efficiency services, the customer should be able to opt-out of sharing with the third party.
- A third party receives energy usage information from the utility, but does not provide services on behalf of the utility. Disclosure to this third party should require express, prior, written authorization, in a form we describe in our proposed rules, and the third party should be subject to data security requirements, limits on secondary uses and onward disclosure without consent, and other limits.
- A third party receives energy usage information directly from the customer. The rules we outline should also be extended to these third parties. However, we do not in this filing take a position on what entity should enforce the privacy obligations and commitments of this category of third parties.

II. The Commission Should Implement Specific Policies and Procedures Conforming to the Fair Information Practice (FIPs) Principles It Has Recognized

In convening this privacy proceeding, the Commission has recognized the need to develop privacy rules before permitting third-party access to customer energy data.[11] Adopting privacy rules implementing the full set of FIPs now, at the beginning of Smart Grid deployment, will provide a sound and adaptable framework for designing privacy into the Smart Grid as it develops, giving utilities and innovators a solid framework upon which to build. Building appropriate privacy protections into the Smart Grid now, rather than trying to incorporate them at a later date, will protect customer privacy while reducing future costs for ratepayers and utilities.

[11] Assigned Commissioner's and Administrative Law Judge's Joint Ruling of July 30, 2010 at 5.

A. The Commission Should Implement Requirements for Handling Smart Grid Data Based on the FIPs Framework in Order to Fill Important Privacy Gaps Left By Existing Frameworks, Statutes, and Policies

1. Pure Notice-and-Choice Regimes Are Insufficient for Protecting Customer Privacy

The full FIPs framework includes eight principles: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Data Security, and Accountability and Auditing.[12] Each principle protects a unique and vital aspect of customer privacy. Although the full FIPs framework incorporates elements of notice-and-choice, it also fills serious gaps found in pure notice-and-choice regimes.

Notice-and-choice regimes are premised on the idea that privacy is best protected by informing customers of how their information is being collected and used and by giving them choices based upon that information. These are important and essential values. However, notice-and-choice alone has proved insufficient to protect privacy in real-world situations. As recently noted by a Commerce Department official, "[t]here are essentially no defenders anymore of the pure notice-and-choice model."[13] Customers rarely read privacy notices issued by companies, largely due to the length and complexity of those policies.[14] Even if customers do read privacy policies, most are "essentially unusable as decision-making aids,"[15] either because they are difficult to understand,[16] or because the service itself is conditioned upon consent to their contents. This failure reflects the privacy policies themselves, not customer apathy. When customers learn how their information is collected and used, they are concerned

---

[12] *See, e.g.,* Joint Comments of CDT and EFF (March 9, 2010), supra note 7 at 15-22 (describing the full set of FIPs in greater detail).

[13] Lohr, *supra* note 8, at BU4.

[14] *See* Aleecia M. McDonald & Lorrie F. Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP (2008), *available at* http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf at 2.

[15] Carlos Jensen & Colin Pitts, *Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices*, 6 Proceedings of the SIGCHI conference on human factors in computing systems 471, 477 (2004), *available at* http://delivery.acm.org/10.1145/990000/985752/p471-jensen.pdf .

[16] *See* An Interview with David Vladeck of the F.T.C., N.Y. TIMES, Aug. 5, 2009, *available at* http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc ("Disclosures are now written by lawyers, they're 17 pages long. I don't think they're written principally to communicate information; they're written defensively…. And I don't believe that most consumers either read them, or, if they read them, really understand it.").

and want more control.[17] Indeed, the Federal Trade Commission (FTC) has begun to file actions of deceptive business practices against firms employing insufficient policies based on notice-and-choice.[18] As the FTC's Director of Consumer Protection recently noted, "I'm not sure that consent really reflects a volitional, knowing act."[19] In sum, experts agree that notice and choice alone are insufficient to safeguard customer privacy.

2. Concrete Policy Requirements Based on the FIPs are Necessary in Order to Fill Existing Statutory Gaps Governing Utilities and Third Parties and to Provide a Clear, Comprehensive Framework to Protect Customer Privacy

In California, a number of regulations govern the privacy practices of utilities and third parties involved in Smart Grid deployment. This regulatory web provides partial safeguards for customer privacy but also includes gaps that leave customers vulnerable. California Public Utilities Code § 394 provides that electrical service providers keep confidential "customer specific billing, credit, or usage information,"[20] but varies by type of service provider in its protections, in its guidance on the type of notice that must be provided,[21] and overall, does not provide a comprehensive guiding framework under which service providers can operate.

More generally, California's Business and Professions Code requires online posting of privacy policies and that certain content be included in those privacy policies, but the content requirements are quite limited, and all requirements apply only to operators of commercial websites and online services.[22] California's Information Practices Act of 1977, which is

---

[17] *See e.g.,* Scott Cleland, *Americans Want Online Privacy – Per New Zogby Poll* (June 9, 2010), *available at* http://precursorblog.com/content/americans-want-online-privacy-new-zogby-poll.

[18] *See In the Matter of Sears Holdings Management Corporation*, FTC File No. 082 3099, *available at*: http://www.ftc.gov/opa/2009/09/sears.shtm (arguing that even full disclosure of its practices was deceptive when buried in a "lengthy user license agreement, available to consumers at the end of a multi-step registration process").

[19] *See* An Interview with David Vladeck of the F.T.C., *supra* note 16.

[20] 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.").

[21] CAL. PUB. UTIL. CODE § 394.5 (minimum requirements in notice to potential customers); CAL. PUB. UTIL. CODE § 394.4(d) (notices must be "easily understandable").

[22] BUS. & PROF. CODE § 22575 (requiring privacy policies to be posted by operators of Web sites or online services who collect "personally identifiable information").

intended to protect the privacy of individuals by regulating the maintenance and dissemination of personal information[23] by businesses or agencies,[24] at times only protects personal information that can be linked directly to a customer's name.[25] California also mandates customer notification in case of data breaches, but only where certain categories[26] of unencrypted personal information are computerized, and only where it "was, or is reasonably believed to have been, acquired by an unauthorized person."[27] Similarly, the latest addition to the Public Utilities Code, section 8380 (previously Senate Bill 1476),[28] provides some minimal protections to energy usage data, but does not go far enough towards protecting customers from unwanted secondary uses of their data.[29]

Overall, California has a welter of regulations concerning privacy, some of which applies to Smart Grid entities. However, this patchwork creates neither comprehensive protection for customers nor a clear framework for Smart Grid entities to follow in protecting customers' information. It is to the benefit of customers, and all Smart Grid entities, for the Commission to adopt such a clear framework.

---

[23] *See* CAL. CIVIL CODE § 1798.1(a) ("The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies."); CAL. CIV. CODE § 1798.1(b) ("The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.").

[24] *See* CAL. CIV. CODE § 1798.14-1798.24.b; CAL. CIV. CODE § 1798.80-1798.84.

[25] CAL. CIV. CODE § 1798.81.5(d)(1); CAL. CIV. CODE § 1798.82(e); CAL. CIV. CODE § 1798.29(e).

[26] CAL. CIV. CODE § 1798.82(e) ("'[P]ersonal information' means an individuals first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number; (2) Drivers license number or California Identification Card number; (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (4) Medical information; (5) Health insurance information."

[27] CAL. CIV. CODE § 1798.82(a); § 1798.29(a).

[28] *See* Senate Bill No. 1476, Chapter 497, Statutes of 2010, *available at* http://www.leginfo.ca.gov/pub/09-10/bill/sen/sb_1451-1500/sb_1476_bill_20100929_chaptered.pdf.

[29] *See Id*.

3. Present Privacy Policies of Utilities and Third Parties Are Insufficient to Protect Customer Privacy in Smart Grid Data

A limited review of current privacy policies for energy data suggests that traditional notice practices may have been sufficient in the past, but are no longer able to fully protect customers in the Smart Grid environment. It is more important than ever that companies have readily accessible written policies regarding energy usage data that specifically identify the purposes of data collection and the specific entities to which data is disclosed. Unfortunately, many companies today do not have readily accessible policies.[30] Moreover, where relevant policies are available, they are often underspecified—lacking, for example, definitions for critical terms, such as the types of energy usage data protected.[31] Few current policies provide users with granular controls, and most give users only the option to cancel service, rather than the opportunity to make meaningful choices about their data use.[32] Although policies often list purposes for which data will be used, those purposes are often so broadly stated (e.g., "to provide you with a better experience")[33] as to allow virtually limitless uses of the data. No energy service policy that we were able to collect explains whether the information collected from customers is limited to the minimum amount needed to fulfill any stated purpose, or mentions remedial procedures for managing data breaches or other security violations. Thus,

---

[30] We sought to collect privacy policies concerning energy usage data and/or web usage data from PG&E, SCE, SDG&E and Google PowerMeter. We were unable to access energy data polices for two of the three IOUs: SDG&E has a privacy policy for only web usage, *available at* http://www.sdge.com/privacy/; SCE has a privacy policy for only web usage, *available at* http://www.sce.com/PrivacyPolicy/. We requested, but were unable to obtain prior to this filing, SDG&E's and SCE's policies related to *energy data or services*. PG&E, however, does provide an easily accessible policy covering energy data or services on its website, *available at* http://www.pge.com/about/company/privacy/customer. We look forward to reviewing others' policies as part of this proceeding.

[31] *E.g.*, PG&E's privacy policy interchangeably uses the terms "customer information," "personal information," "personally identifiable information," and "personal customer information" without defining those terms, *available at* http://www.pge.com/about/company/privacy/customer.

[32] *E.g.*, neither Google PowerMeter's nor PG&E's policy allows users to opt-out of any parts of the policy except through cancellation, *available at* http://www.google.com/powermeter/privacy and http://www.pge.com/about/company/privacy/customer.

[33] Google Privacy Policy (effective date Oct. 3, 2010), *available at* http://www.google.com/privacypolicy_2010.html (stating that it may use data to "to provide you with a better experience and to improve the quality of our services"); see also PG&E's Privacy Policy, *available at* http://www.pge.com/about/company/privacy/customer (stating that it may use data "to manage, provide, and improve our services and business operations").

under the present circumstances, even diligent customers may not understand the notice provided; if they do, existing policies are unlikely to provide them with meaningful choices. These inadequacies illustrate the practical outcomes of the regulatory gaps that the Commission needs to fill in order to ensure that customer privacy is protected in the Smart Grid.

III. The Appendix Offers a Clear, Reasonable and Effective Implementation of the FIPs for the Smart Grid

To be effective, the FIPs principles must take concrete form. Only then will all of the parties—customers, utilities, and third parties—tangibly understand their rights and responsibilities. As such, in response to the Ruling's request for specific policies and procedures,[34] we recommend to the Commission and the stakeholders the specific requirements attached hereto as Appendix A.

Our proposal improves on the traditional notice and consent model in important ways. Under "Transparency" and "Purpose Specification," it ensures that customers will receive *specific* information about who collects, receives, stores, or uses their data, and for what purposes each entity uses the data. Under the principle of "Individual Participation," it affirms customers' right to access their own data and to challenge its accuracy. Our proposal draws a distinction between primary purposes and secondary purposes, and ties use and disclosure limits to those concepts, making it clear that utilities do not need consent to collect, retain, or use data for purposes directly related to the provision of electrical or gas service to the customer, but that prior express authorization is needed for disclosure to third parties not providing service on behalf of the utility and for other secondary uses.[35] In a vast improvement over many current privacy policies, we make it clear that customer consent is specific to each third party and to each purpose. As noted by Southern California Edison at the Commission's joint event with the National Institute of Standards and Technology on September 29, genuine choice on secondary

[34] Ruling of September 27, 2010 at 6.

[35] SB 1476 contemplates that energy usage data may be disclosed with customer consent for secondary commercial purposes. Our proposed rules specify how such consent should be obtained. However, SB 1476 does not define secondary commercial uses, nor does it suggest that the concept is limitless. The Commission may address whether some secondary commercial purposes should be precluded entirely.

uses is especially important in the energy context, where customers rarely have a choice in the entity providing power.[36]

In another improvement, under "Data Minimization," the proposal ties the amount of data collected and disclosed to the specified purposes, in order to minimize the amount of unnecessary customer data collected or disclosed by utilities and third parties.[37]

Finally, the proposal addresses disclosure pursuant to legal process[38] and requires reasonable security protections and basic accountability.

In developing the proposal, we have attempted to protect the privacy of customers and provide clear standards without placing undue burden on Smart Grid service providers. We invite parties to this proceeding to endorse our proposal or to provide us with suggestions for improvement, both in the upcoming workshops and in the reply comments.

IV. Conclusion

The Center for Democracy & Technology and the Electronic Frontier Foundation commend the Commission on its careful consideration of the customer privacy risks presented by the emerging Smart Grid. We urge the Commission to adopt the policies and procedures set

---

[36] *See* archived video of NIST/CPUC Co-Sponsored Event on Cyber-Security and Privacy (September 29, 2010), *available at* http://www.californiaadmin.com/cpuc.shtml.

[37] While our recommendation focuses on a rule-oriented framework for data minimization, the flow of energy usage data from the home can also be minimized by the very design or architecture of consumer energy management systems. We thus urge the Commission to recognize that "it is possible to protect consumer privacy at a macro level by choosing a system design that minimizes frequent access to granular data from outside the consumer site" and to seek information from parties to this proceeding about such possibilities. *See* NISTIR 7628, GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 36-37 (Aug. 2010) (using the example of intelligent gateways that can both optimize energy consumption and prevent pattern recognition against known load profiles).

[38] The proposal, in accordance with existing law, directs covered entities, in the absence of consent, not to disclose energy usage data except pursuant to a warrant or court order. While our proposal does not separately address standards for government access in criminal investigations versus standards for access in civil litigation, we believe that in cases where very detailed data is being sought in the course of a criminal investigation, a warrant will be required. The Supreme Court, in *Kyllo v. United States*, 533 U.S. 27 (2001) held that a warrant is required to use an infrared device to collect what is in essence energy usage data (the heat signature of a home), where the information being collected was detailed enough to permit inferences about what was going on inside the home. Justice Scalia, in writing for the majority, stated: "In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes. Thus, in *Karo*, *supra*, the only thing detected was a can of ether in the home; and in *Arizona* v. *Hicks*, 480 U.S. 321 (1987), the only thing detected by a physical search that went beyond what officers lawfully present could observe in "plain view" was the registration number of a phonograph turntable. These were intimate details because they were details of the home, just as was the detail of how warm—or even how relatively warm—Kyllo was heating his residence." *Kyllo* at 37-38.

out in the Appendix. These proposals implement the full set of FIPs that the Commission has recognized as critical to safeguarding customer privacy. We respectfully request an opportunity to discuss these proposals in the upcoming workshops on October 26 and 27. Implementation of this proposal will support development of the Smart Grid in California and serve as a model for the rest of the nation.

Respectfully submitted this October 15, 2010 at San Francisco, California.

/s/ Jennifer Urban

JENNIFER URBAN, Attorney
Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley School of Law
585 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7338
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 – Privacy Policies and Procedures

1. DEFINITIONS

(a) **Covered Entity.** A "covered entity" is (1) any electrical service provider, electric corporation, gas corporation or community choice aggregator, or (2) any third party that collects, stores, uses, or discloses covered information [relating to 100 or more households or residences].[39]

(b) **Covered Information.** "Covered information" is any energy usage information concerning an individual, family, household, or residence, except that covered information does not include information from which identifying information has been removed such that it cannot reasonably be identified or re-identified with an individual, family, household, or residence.

(c) **Primary Purposes.** The "primary purposes" for the collection, storage, use or disclosure of covered information are to—
   (1) provide or bill for electrical power,
   (2) fulfill other operational needs of the electrical system or grid, and
   (3) implement demand response, energy management, or energy efficiency programs operated by, or on behalf of and under contract with, an electric or gas corporation.

(d) **Secondary Purpose.** "Secondary purpose" means any purpose that is not a primary purpose.

2. TRANSPARENCY (NOTICE)

(a) **Generally.** Covered entities shall provide customers with meaningful, clear, accurate, specific, and comprehensive notice regarding the collection, storage, use, and disclosure of covered information.

(b) **When Provided.** Covered entities shall provide notice in their first paper correspondence with the customer, if any, and shall provide conspicuous posting of the notice on the home page of their website.

(c) **Form.** The notice shall be labeled "Privacy Policy: Notice of Collection, Storage, Use and Disclosure of Energy Usage Information" and shall—
   (1) be written in easily understandable language,
   (2) be no longer than is necessary to convey the requisite information.

(d) **Content.** The notice shall state clearly—
   (1) the identity of the covered entity,
   (2) the effective date of the notice,
   (3) the covered entity's process for altering the notice, including how the customer will be informed of any alterations, and where prior versions will be made available to customers, and
   (4) the title and contact information, including email address, postal address, and telephone number, of an official at the covered entity who can assist the customer with privacy questions, concerns, or complaints regarding the collection, storage, use, or distribution of covered information.

---

[39] Comment: Some further thought needs to be given to the interplay between this threshold and the rules for legal process; we are concerned about unregulated governmental access to energy usage information from landlords of smaller apartment buildings.

3. PURPOSE SPECIFICATION The notice required under section 2 shall provide—

(a) an explicit description of—
  (1) each category of covered information collected, used, stored or disclosed by the covered entity, and, for each category of covered information, the specific purposes for which it will be collected, stored, used, or disclosed, and
  (2) each category of covered information that is disclosed to third parties, and, for each category, (i) the purposes for which it is disclosed, (ii) the identities of the third parties to which it is disclosed, and (iii) the value of the disclosure to the customer;

(b) the periods of time that covered information is retained by the covered entity;

(c) a description of the choices available to customers and the means by which they may exercise those choices, including the means by which they may—
  (1) view, inquire about, or dispute their covered information, and
  (2) limit the collection, use, storage or disclosure of covered information; and

(d) the consequences to the customer, if any, of refusing consent to the covered entity, in whole or in part, regarding the collection, storage, use, or distribution of covered information.

4. INDIVIDUAL PARTICIPATION (ACCESS AND CONTROL)

(a) **Access.** Covered entities shall provide to customers convenient and secure access to their covered information—
  (1) in an easily readable format that is at a level of detail sufficient for the customer to utilize reasonably available energy management or energy efficiency products, but in no event at a level less detailed than that at which the covered entity discloses the data to third parties for demand response, energy management or energy efficiency purposes.
  (2) The Commission shall, by subsequent rule, prescribe what is a reasonable time for responding to customer requests for access.

(b) **Control.** Covered entities shall provide customers with convenient mechanisms for—
  (1) granting and revoking authorization for secondary uses of their covered information,
  (2) disputing the accuracy or completeness of covered information that the covered entity is storing or distributing for any primary or secondary purpose, and
  (3) requesting corrections or amendments to covered information that the covered entity is collecting, storing, using, or distributing for any primary or secondary purpose.

(c) **Disclosure Pursuant to Legal Process.**
  (1) Except as otherwise provided in this rule or expressly authorized by law, a covered entity shall not disclose covered information except pursuant to a warrant or other court order naming with specificity the customers whose information is sought. Unless otherwise directed by a court, covered entities shall treat requests for real-time access to covered information as wiretaps, requiring approval under the federal or state wiretap law.
  (2) Unless otherwise prohibited by court order, a covered entity, upon receipt of a demand for disclosure of covered information, shall, prior to complying, notify the customer in writing and allow the customer 7 days to appear and contest the claim of the person or entity seeking disclosure.
  (3) Nothing in this rule prevents a person or entity seeking energy usage information from demanding such information from the customer under any applicable legal procedure or authority.

(4) Nothing in this section prohibits a covered entity from disclosing covered information with the consent of the customer, where the consent is express, written and specific to the purpose and to the person or entity seeking the information.
(5) Nothing in this rule prevents a covered entity from disclosing, in response to a subpoena, the name, address and other contact information regarding a customer.
(6) On an annual basis, covered entities shall report to the Commission the number of times that customer data has been sought without consent, and for each such instance, whether it was a civil or criminal case, whether the covered entity complied with the request as initially presented or as modified in form or scope, and how many customers' records were disclosed. The Commission should make such reports publicly available.

5. DATA MINIMIZATION

(a) **Generally.** Covered entities shall collect, store, use, and disclose only as much covered information as is necessary to accomplish a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.
(b) **Data Retention.** Covered entities shall maintain covered information only for as long as necessary to accomplish a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.
(c) **Data Disclosure.** Covered entities shall not disclose to any third party more covered information than is necessary to carry out on behalf of the covered entity a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

6. USE AND DISCLOSURE LIMITATION

(a) **Generally.** Covered information shall be used solely for the purposes specified by the covered entity in accordance with section 3.
(b) **Primary Purposes.** A gas or electric corporation may use covered information for primary purposes without customer consent.
(c) **Disclosures to Third Parties.** A gas or electric corporation may disclose covered information to a third party when the third party is performing a primary purpose on behalf of a gas or electrical corporation, provided that the gas or electric corporation shall, by contract, require the third party to collect, store, use, and disclose covered information under policies and practices no less protective than those under which the gas or electric corporation itself operates and, if the information is being disclosed for demand response, energy management or energy efficiency purposes, the gas or electric corporation permits customers to opt-out of such disclosure.
(d) **Secondary Purposes**. No covered entity shall use or disclose covered information for any secondary purpose without obtaining the customer's prior, express, written authorization for each such purpose, provided that authorization is not required when information is—
    (1) provided to a law enforcement agency in response to lawful process;
    (2) required by the Commission pursuant to its jurisdiction and control over electric and gas corporations.
(e) **Customer Authorization.**
    (1) **Authorization.** Separate authorization must be obtained for each secondary purpose.

(2) **Revocation.** Customers have the right to revoke, at any time, any previously granted authorization.
(3) **Expiration.** Customer consent shall be deemed to expire after two years, after which time customers will need to reauthorize any secondary purposes.

(f) **Parity.** Covered entities shall permit customers to cancel authorization for any secondary use of their covered information by the same mechanism initially used to grant authorization.

7. DATA QUALITY AND INTEGRITY

Covered entities shall ensure that covered information they collect, store, use, and disclose is accurate and complete.

8. DATA SECURITY

(a) **Generally.** Covered entities shall implement appropriate administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure.

(b) **Breach.** Covered entities shall disclose any breach in accordance with section 1798.82 of the Information Practices Act. In addition, covered entities shall notify the Commission of breaches of covered information.

9. ACCOUNTABILITY AND AUDITING

(a) **Generally**. Covered entities shall be accountable for complying with the principles herein, and must file with the Commission—
(1) the privacy notices that they provide to customers,
(2) their internal privacy and security policies,
(3) the identities of agents, contractors and other third parties to which they disclose covered information, the purposes for which that information is disclosed, indicating for each category of disclosure whether it is for a primary purpose or a secondary purpose, and
(4) copies of any secondary-use authorization forms by which the covered party secures customer authorization for secondary uses of covered data.

(b) **Redress.** Covered entities shall provide customers with mechanisms for appropriate access to covered information, for correction of inaccurate covered information, and for redress in the event of a violation of these rules.

(c) **Training**. Covered entities shall provide appropriate training to all employees and contractors who use, store or process covered information.

(d) **Audits**. Covered entities shall conduct an independent audit of security and privacy practices at least once per year to monitor compliance with its privacy and security commitments, and shall report the findings to the Commission.

(e) **Disclosures**. On an annual basis, covered entities shall disclose to the Commission—
(1) the number and identities of authorized third parties accessing customer energy usage information,
(2) the number of security breaches experienced by the electrical corporation or gas corporation, and
(3) the number and percentage of customers affected by breaches of covered information.

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, PROPOSED SMART GRID PRIVACY POLICIES AND PROCEDURES - OPENING RESPONSE OF THE CENTER FOR DEMOCRACY & TECHNOLOGY AND THE ELECTRONIC FRONTIER FOUNDATION TO ASSIGNED COMMISSIONER'S RULING OF SEPTEMBER 27, 2010, 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 October 15, 2010 at Berkeley, California

/s/ Heather Patterson
HEATHER PATTERSON, Clinical Intern
Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley School of Law
585 Simon Hall
Berkeley, CA 94720-7200

SERVICE LIST

martinhomec@gmail.com
carlgustin@groundedpower.com
vladimir.oksman@lantiq.com
jandersen@tiaonline.org
jeffrcam@cisco.com
dbrenner@qualcomm.com
coney@epic.org
michael.sachse@opower.com
cbrooks@tendrilinc.com
SDPatrick@SempraUtilities.com
npedersen@hanmor.com
slins@ci.glendale.ca.us
douglass@energyattorney.com
xbaldwin@ci.burbank.ca.us
kris.vyas@sce.com
ATrial@SempraUtilities.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
elaine.duncan@verizon.com
pickering@energyhub.net
margarita.gutierrez@sfgov.org
lms@cpuc.ca.gov
fsmith@sfwater.org
srovetti@sfwater.org
tburke@sfwater.org
marcel@turn.org
mkurtovich@chevron.com
cjw5@pge.com
david.discher@att.com
nes@a-klaw.com
harold@seakayinc.org
pcasciato@sbcglobal.net
steven@sfpower.org
tien@eff.org
jarmstrong@goodinmacbride.com
mgo@goodinmacbride.com
mday@goodinmacbride.com
ssmyers@worldnet.att.net
judith@tothept.com
lex@consumercal.org
farrokh.albuyeh@oati.net
Service@spurr.org
Mark.Schaeffer@granitekey.com
wbooth@booth-law.com
lencanty@blackeconomiccouncil.org
jwiedman@keyesandfox.com
kfox@keyesandfox.com
gmorris@emf.net
robertginaizda@gmail.com
enriqueg@greenlining.org
aaron.burstein@gmail.com
dkm@ischool.berkeley.edu
longhao@berkeley.edu
jurban@law.berkeley.edu
kerry.hattevik@nrgenergy.com
rquattrini@energyconnectinc.com
michael_w@copper-gate.com
TGlassey@Certichron.com
seboyd@tid.org
dzlotlow@caiso.com
dennis@ddecuir.com
scott.tomashefsky@ncpa.com
jhawley@technet.org
lnavarro@edf.org
Lesla@calcable.org
cbk@eslawfirm.com
mcoop@homegridforum.org
cassandra.sweet@dowjones.com
dblackburn@caiso.com
diana@aspectlabs.com
gstaples@mendotagroup.net
jlin@strategen.com
MNelson@MccarthyLaw.com
ryn@rynhamiltonconsulting.com
stephaniec@greenlining.org
tam.hunt@gmail.com
ttutt@smud.org
mrw@mrwassoc.com
EGrizard@deweysquare.com
jon.fortune@energycenter.org
martinhomec@gmail.com

mokeefe@efficiencycouncil.org
r.raushenbush@comcast.net
sephra.ninow@energycenter.org
sue.mara@rtoadvisors.com
kladko@aspectlabs.com
ep@aspectlabs.com
john.quealy@canaccordadams.com
mark.sigal@canaccordadams.com
barbalex@ctel.net
crjohnson@lge.com
smaye@nappartners.com
julien.dumoulin-smith@ubs.com
david.rubin@troutmansanders.com
jennsanf@cisco.com
marybrow@cisco.com
jmccarthy@ctia.org
jay.birnbaum@currentgroup.com
puja@opower.com
bboyd@aclaratech.com
bob.rowe@northwestern.com
monica.merino@comed.com
sthiel@us.ibm.com
ann.johnson@verizon.com
ed.may@itron.com
rgifford@wbklaw.com
leilani.johnson@ladwp.com
GHealy@SempraUtilities.com
jorgecorralejo@sbcglobal.net
dschneider@lumesource.com
lmitchell@hanmor.com
david@nemtzow.com
cjuennen@ci.glendale.us
mark.s.martinez@sce.com
case.admin@sce.com
janet.combs@sce.com
michael.backstrom@sce.com
nquan@gswater.com
Jcox@fce.com
esther.northrup@cox.com
KFoley@SempraUtilities.com
mike@ucan.org
kmkiener@cox.net
djsulliv@qualcomm.com
HRasool@SempraUtilities.com
TCahill@SempraUtilities.com
CManson@SempraUtilities.com
DNiehaus@SempraUtilities.com
CentralFiles@SempraUtilities.com
jerry@enernex.com
traceydrabant@bves.com
peter.pearson@bves.com
dkolk@compenergy.com
ek@a-klaw.com
rboland@e-radioinc.com
juan.otero@trilliantinc.com
mozhi.habibi@ventyx.com
faramarz@ieee.org
rudy.reyes@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
regrelcpuccases@pge.com
dpb5@pge.com
DNG6@pge.com
filings@a-klaw.com
Kcj5@pge.com
mpa@a-klaw.com
rcounihan@enernoc.com
sls@a-klaw.com
stephen.j.callahan@us.ibm.com
tmfry@nexant.com
info@tobiaslo.com
BKallo@rwbaird.com
bcragg@goodinmacbride.com
bdille@jmpsecurities.com
jscancarelli@crowell.com
jas@cpdb.com
joshdavidson@dwt.com
nml@cpdb.com
salleyoo@dwt.com
SDHilton@stoel.com
suzannetoller@dwt.com
dhuard@manatt.com
mariacarbone@dwt.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
ralf1241a@cs.com
john_gutierrez@cable.comcast.com
mike.ahmadi@Granitekey.com
sean.beatty@mirant.com
lewis3000us@gmail.com
Douglas.Garrett@cox.com
rstuart@brightsourceenergy.com
nellie.tong@us.kema.com
Valerie.Richardson@us.kema.com
cpucdockets@keyesandfox.com
dmarcus2@sbcglobal.net
rschmidt@bartlewells.com
RobertGnaizda@gmail.com
samuelk@greenlining.org
jskromer@qmail.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
davidmorse9@gmail.com
e-recipient@caiso.com
aivancovich@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
jfine@edf.org
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
pkulkarn@energy.state.ca.us
lmh@eslawfirm.com
abb@eslawfirm.com
bsb@eslawfirm.com
glw@eslawfirm.com
jparks@smud.org
ljimene@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
sas@a-klaw.com
wmc@a-klaw.com
bschuman@pacific-crest.com
sharon.noell@pgn.com
TRH@cpuc.ca.gov
ahl@cpuc.ca.gov
ag2@cpuc.ca.gov
agc@cpuc.ca.gov
am1@cpuc.ca.gov
crv@cpuc.ca.gov
df1@cpuc.ca.gov
dbp@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
ltt@cpuc.ca.gov
lbs@cpuc.ca.gov
lau@cpuc.ca.gov
zaf@cpuc.ca.gov
mjd@cpuc.ca.gov
mzx@cpuc.ca.gov
mbp@cpuc.ca.gov

mc3@cpuc.ca.gov
wtr@cpuc.ca.gov
rhh@cpuc.ca.gov
srt@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