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) Phase III Energy Data Center

M E M O R A N D U M

To: Participants of Working Group organized pursuant to Administrative Law Judge's Ruling Setting Schedule To Establish "Data Use Cases," Timelines For Provision Of Data, And Model Non-Disclosure Agreements, from Rulemaking Proceeding No. 08-12-009

From: Electronic Frontier Foundation and the Samuelson Law, Technology & Public Policy Clinic at the University of California, Berkeley, School of Law

Date: April 1, 2013

Re: Legal Considerations for Smart Grid Energy Data Sharing

INTRODUCTION

This memorandum is one of two memoranda offered by the Electronic Frontier Foundation (EFF) and the Samuelson Law, Technology & Public Policy Clinic at the University of California, Berkeley, School of Law to aid in the parties' discussions during the Working Group meetings outlined in Judge Sullivan's February 27, 2013 ruling, titled *Administrative Law Judge's Ruling Setting Schedule to Establish "Data Use Cases," Timelines for Provision of Data, and Model Non-Disclosure Agreements* ("Ruling").

This memorandum covers legal background relevant to this proceeding, providing a brief explanation of important laws that apply to energy usage data sharing, as well as a brief background of the legal landscape covered in the proceeding to date. The other memorandum, titled *Technical Issues with Anonymization & Aggregation of Detailed Energy Usage Data as Methods for Protecting Customer Privacy*, offers some technical background on aggregation and

anonymization models for protecting privacy.

The proceeding thus far has established both basic principles and a targeted legal framework—in the form of the Rules Regarding Privacy and Security Protections for Energy Usage Data ("Privacy Rules"),[1] adopted by the California Public Utilities Commission ("Commission") in D. 11-07-056 ("2011 Decision")[2] and set forth in Attachment D to that Decision—for managing customer data collected by smart meters. In 2012 the Privacy Rules were extended to customers of gas corporations, community choice aggregators, as well as residential and small commercial customers of electric service providers.[3] It now presents an opportunity to apply this framework in establishing effective, secure protocols for more streamlined access to the rich and highly sensitive information captured by smart meters.

Following the Ruling, the Working Group is expected to discuss definitions of "aggregate" and "anonymous" data, as well as standards for achieving optimal aggregation or anonymization and reasonable protocols for sharing those categories of data. In order to fulfill these goals, Working Group participants must have the legal landscape on which we are operating firmly in hand. Further, understanding the legal contours of smart grid data sharing will enable more productive discussions of the validity and/or scope of the proposed "use cases" set out in the Ruling.

DISCUSSION

During this proceeding, the Commission has established that smart grid data can reveal a great deal of private information about life inside a premises, including: how many inhabitants are home or away at a given time; when those inhabitants go to bed, wake up, take showers, or cook dinner; and what devices inhabitants use, including personal medical devices.[4] Known privacy and security risks include, among others:

---

[1] *Rules Regarding Privacy and Security Protections for Energy Usage Data*, in *Attachment D*, Decision Adopting Rules to Protect The Privacy And Security of the Electricity Usage Data of the Customers of Pacific Gas & Electric Company, Southern California Edison Company, And San Diego Gas & Electric Company, Rulemaking 08-12-009 (July 29, 2011) ["Privacy Rules"].

[2] Decision Adopting Rules to Protect The Privacy And Security of the Electricity Usage Data of the Customers of Pacific Gas & Electric Company, Southern California Edison Company, And San Diego Gas & Electric Company, Rulemaking 08-12-009 (July 29, 2011) ["2011 Decision"].

[3] D. 12-08-045 (August 23, 2012).

[4] *See* Statement from Martin Pollock of Siemens Energy, in Gerard Wynn, *Privacy Concerns Challenge Smart Grid Rollout*, REUTERS, June 25, 2010, *available at*: http://uk.reuters.com/article/idUKTRE65O1RQ20100625. *See also*

- Data breach (hacking) or data leaks (inadvertent disclosure to the public);
- Re-identification of aggregated and/or anonymized data to reveal personally-identifying information; and
- "Mission creep," the potential future expansion of access to energy usage data to include additional users or uses of the data beyond what was initially contemplated (e.g., for law enforcement).

This proceeding has also already established the applicability of a variety of laws intended to protect Californians' data privacy interests. Many of these laws are already discussed in the 2011 Decision and are reflected in the Privacy Rules. In the Privacy Rules phase of the proceeding and in his presentation at the January 15th Workshop, Chris Warner of Pacific Gas & Electric provided a list of the laws and regulations relevant to the collection, maintenance, use, and disclosure of smart grid data.[5] Additionally, in its Opening Comment on the Proposed Energy Data Center ("EDC"), EFF raised questions regarding the applicability of existing state law, including the Information Practices Act of 1977 ("IPA"),[6] to EDC proposals. Parties participating in the January 15th and 16th Workshops identified as the IPA as a relevant topic for further review.[7]

To aid this phase of the proceeding, this memorandum further discusses some of these laws as applied to the disclosure of customer energy usage data. Specifically, it briefly reviews the California Constitution, the Fair Information Practices Principles ("FIPPs"), and Public Utilities Code Section 8380 (commonly referred to as "SB 1476") as important foundations for the Privacy Rules. It then provides further review of the IPA and its applicability to agency sharing of energy usage data. Finally, the memorandum reviews for the Working Groups the key provisions of the Privacy Rules themselves, which implement SB 1476, other relevant law, and the FIPPs for smart meter data. With a foundational understanding of these laws, the Working Groups will be better equipped to devise solutions for smart grid data sharing that comply with these existing laws.

Mikhail A. Lisovich, Deirdre K. Mulligan & Stephen B. Wicker, *Inferring Personal Information from Demand-Response Systems*, IEEE SECURITY & PRIVACY (Jan.–Feb. 2010).

[5] *Appendix A: List of Current Statutes, Regulations, Decisions and Protocols Related to Customer Privacy Applicable to California Energy Utilities*, Attachment B from Ruling D. 11-07-056; Slide presentation by Christopher J. Warner, *Existing Energy Data Sharing Protocols: A Potential Consensus Approach*, CPUC Workshop (Jan. 15, 2013), *available at* ftp://ftp.cpuc.ca.gov/13011516_EgyDataWorkshop/.

[6] Opening Comments of the Electronic Frontier Foundation, at 10–11 (Dec. 17, 2012) [hereinafter EFF Opening Comment].

[7] Slide presentation by Christopher J. Warner, *Existing Energy Data Sharing Protocols: A Potential Consensus Approach*, CPUC Workshop (Jan. 15, 2013), *available at* ftp://ftp.cpuc.ca.gov/13011516_EgyDataWorkshop/.

Before commencing the Working Groups, participants should understand that these laws require us to propose definitions and implement "use case" solutions that are dynamic and adaptable. This is because the legal landscape governing data sharing varies—and can change dramatically—depending on a number of factors: (1) the identity of the data custodian; (2) the identity of the data requester; (3) the purpose of the data disclosure; and (4) the level of granularity of the data requested. The proposed use cases represent different permutations of these variables, so the law necessarily treats them differently. Understanding the legal obligations that attach to each data-sharing scenario will enable more accurate evaluation and more effective problem-solving.

A. California Law

1. The California Constitution

Article I, Section 1 of the California Constitution recognizes each individual's right to privacy. There is general agreement among the judicial, scholarly, legislative, and regulatory communities that the data collected by smart meters reveals intimate details about the lives of California citizens. As such, the California Constitution establishes a baseline obligation to protect energy usage data from harmful disclosure or use.

The same interests that motivated California citizens to enact Section 1 by ballot amendment in 1972 still apply today: (1) the overbroad collection and retention of unnecessary personal information by government and business interests; and (2) 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.[8]

Representative of the high value the California public places on privacy, the California Constitution imposes an obligation to protect consumer privacy on all parties—including private parties—engaging in smart grid data sharing. As such, addressing privacy issues are necessarily central to this proceeding, and Working Group participants should bear in mind adequate protections against unauthorized use or disclosure of personal information when addressing definitions and use cases.

/

[8] *White v. Davis*, 13 Cal. 3d 757, 775 (1975).

2. Information Practices Act

The IPA (California Civil Code section 1798 *et seq.*) governs the manner in which state agencies, as defined in the IPA, disclose personally identifiable data that they collect and maintain. The statute applies to state-wide agencies, including the Commission and the California Energy Commission (CEC).[9] Should the Commission designate one of these agencies as a custodian of smart grid data, the IPA will apply to that agency's disclosure of the data.

The IPA protects energy usage data that "identifies or describes an individual"—in this context, an individual utility customer.[10] The IPA offers a non-exhaustive list of example types of "personal information" that might be used to identify or describe an individual, including an individual's "name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history."[11] At the January Workshop, Professor Ashwin Machanavajjhala asserted that additional types of information, such as sex, birthdate, and zip code, operate as "quasi-identifiers," capable of re-identifying an individual when linked to other available data. The IPA's open-ended list of identifiers would include that information as well.

As a general rule, state agencies are not permitted to disclose any personal information "in a manner that would link the information disclosed to the individual to whom it pertains."[12] However, a number of exceptions apply, subject to varying protocols and approval procedures depending on the data recipient. For example, Section 1798.24 authorizes disclosure of an individual's personal data in the following pertinent scenarios, among others:

- With the prior written voluntary consent of the individual, Cal. Civ. Code § 1798.24(b);
- To persons, or another state agency, such as the CEC, for whom the information is necessary to fulfill statutory duties, Cal. Civ. Code § 1798.24(e);
- Where the CPUC is required by law to disclose the information to a local government (or federal government) entity,[13] Cal. Civ. Code § 1798.24(f);
- Disclosure to a researcher, if (1) he provides assurance that the information will be used solely for statistical research or reporting purposes, and (2) he does not

[9] Cal. Civ. Code § 1798.3.
[10] Cal. Civ. Code § 1798.3(a).
[11] The IPA also includes "statements made by, or attributed to, the individual" within its list of identifiers. Cal. Civ. Code § 1798.3(a).
[12] Cal. Civ. Code § 1798.24.
[13] We note that there are two separate exceptions relating to warrant and subpoena requirements.

receive the information in a form that will identify the individual, Cal. Civ. Code § 1798.24(h); and

- Disclosure to a researcher within the University of California system, provided that the request is approved by the Committee for the Protection of Human Subjects, Cal. Civ. Code § 1798.24(t).

Of particular relevance to Working Group discussion is Section 1798.24(h), which specifically addresses disclosure for research purposes. This provision underscores the California legislature's commitment to protecting the privacy of the individual(s) to whom the data pertains by explicitly limiting disclosure of personally identifiable information to researchers, while allowing research. We additionally note that Section 1798.24(e) also practically limits the scope of agency disclosures to only those specifically and directly authorized by statute, lest the exception swallow the rule.

One of the fundamental privacy concerns motivating the enactment of the IPA was the risk of data breach, a problem that is prevalent and well-documented among all institutions, including California institutions. An important obligation the IPA imposes on third party data recipients working within the University of California system is that requests for disclosure of personal information must first be approved by the Committee for the Protection of Human Subjects (CPHS), or another institutional review board that has written authorization from the CPHS. Although Section 1798(t) appeared in the original 1977 version of the statute, the specific language requiring approval from the CPHS was added in 2005 to ensure that the UC satisfies minimum standards for data security.[14]

This amendment responds to a high-profile computer hacking incident and data breach that occurred in August 2004, in which a UC Berkeley researcher inadvertently disclosed names, addresses, social security numbers, birthdates, and phone numbers for nearly 1.3 million people residing in California.[15] Data breaches continue to plague the UC system, giving credence to the state legislature's concern about security protocols at public research institutions. For example, in December 2006, UCLA alerted approximately 800,000 current and former students, faculty,

[14] *See* Stats. 2005, c. 241 (S.B. 13) § 1 ("The Legislature recognizes the research community has legitimate needs to access personal information to carry out research . . . the provisions of this bill are not intended to impede research but rather to require and set minimum standards for careful review and approval of requests.").

[15] EFF Opening Comment, at 11. *See also* Senate Bill Analysis, Third Reading, Stats. 2005, c. 241 (S.B. 13) (Aug. 17, 2005). In that case, the researcher requested data from the Department of Social Services (DSS) about participants in the In-Home Supportive Services (IHSS). Although the researcher needed only a random sample of IHSS data, the DSS made the entire IHSS database available for download. Shortly thereafter, a hacker broke into the researcher's computer system, causing a massive data breach.

and staff that a sophisticated computer hacker had broken into its systems and accessed a restricted database containing their personal information.[16] More recently, in 2011, the UCLA Health System notified over 16,000 patients that their names, birthdates, addresses, and medical information had been stolen during the burglary of a physician's home.[17] Although the physician had stored the data on an encrypted external hard drive, the password for the hard drive was written on a piece of paper kept near the computer that was found missing after the incident.

As such, the IPA provides both legal requirements binding on relevant agencies and overall guidance as to how California has thus far approached data risks for California citizens. Accordingly, although the IPA is not binding on utility companies, academic or local government researchers, or other parties who cannot be characterized as state agencies, it nevertheless provides useful guidance in this situation because it approximates how California law might treat the disclosure of energy usage data more generally.

B. The Privacy Rules

In the smart grid context, statewide concern in California with consumer privacy has culminated in the Commission's adoption of the Privacy Rules, which specifically address the sharing of energy usage data held by investor-owned utilities ("IOUs"). The Privacy Rules most directly address the type of data sharing at issue in this phase of the proceeding: (1) they specifically regulate energy usage data collected by smart meters, and (2) they concern disclosure by the IOUs to third party data requesters. As such, they provide the governing general authority on energy usage data sharing by the IOUs.

Accordingly, the Privacy Rules are the primary source of legal guidance as the Working Groups determine how to manage any disclosure of such data, and comprise the central feature of our discussion on relevant law. Part 1 of this section provides a brief background to the Privacy Rules, adopted in 2011, and their implementation of the provisions of SB 1476 and the FIPPs. This background provides a fuller understanding of the Privacy Rules for those participants not previously involved in the proceeding. Part 2 explains the standards and requirements for disclosure of covered information set forth in the Privacy Rules.

---

[16] *UCLA Warns of Unauthorized Access to Restricted Database*, UCLA NEWSROOM (Dec. 12, 2006), http://newsroom.ucla.edu/portal/ucla/UCLA-Warns-of-Unauthorized-Access-7571.aspx?RelNum=7571.
[17] *UCLA Medical Officials Say Patient Information Data Stolen*, L.A. TIMES BLOG (Nov. 4, 2011), http://latimesblogs.latimes.com/lanow/2011/11/ucla-patient-identification-stolen.html.

1. Brief Background to the Privacy Rules: SB 1476 and the FIPPs

In 2010 the California legislature passed **SB 1476**, now codified as Public Utilities Code Section 8380, to regulate the use and disclosure of utility customer data collected by smart meters. SB 1476 applies both to "electrical corporations and gas corporations." Subject to some exceptions, SB 1476 generally prohibits disclosure of "electrical or gas consumption data . . . available as part of an advanced metering infrastructure, [including] the name, account number, or residence of the customer."[18] Under Section 8380 (b)(1) "an electrical corporation or gas corporation shall not share, disclose, or otherwise make accessible to any third party a customer's electrical or gas consumption data, except as provided in subdivision (e) or upon the consent of the customer." The Privacy Rules implement these restrictions and their exceptions with regard to the IOUs.

In addition to implementing the requirements of SB 1476, the Commission established that the sharing of energy usage data should follow **Fair Information Practice Principles** (FIPPs), a widely accepted international framework for handling electronic information in a privacy-protective manner. In the 2011 Decision, the Commission explicitly adopted the FIPPs as California's policy for smart grid privacy. Thus, the foundational principles set forth in the FIPPs provide guidance to the Working Groups as participants determine how to most effectively implement the Privacy Rules.

The eight principles embodied in the FIPPs can inform privacy discussions in the upcoming Working Groups in a number of ways. For example:

1. *Transparency*: Any new repository of data that is separate from the IOUs would make it more difficult to provide notice to individual utility customers about the use or dissemination of their personal information
2. *Individual Participation*: The Commission should continue to use consent measures to involve individual utility customers in processes for data collection, use, dissemination and maintenance. Unlike typical consumers, many utility customers have no choice when buying energy. As a result, foregoing consent for disclosure is not bargained for in the relationship with the utility.
3. *Purpose Specification*: Requesting parties must be required to specify the purpose underlying the request prior to authorization for disclosure.
4. *Data Minimization*: Only the data actually necessary for the particular purpose identified should be disclosed. The FIPPs' minimization principle helps in developing

[18] Pub. Util. Code § 8380(a).

data handling practices that limit data breach and other risks before they happen, and helps data handlers decide on data needs in an efficient manner.

5. *Use Limitation*: There must be mechanisms to ensure that the disclosure of information is used solely for the specified purpose(s).
6. *Data Quality and Integrity*: If multiple parties were permitted to collect and store energy usage data, it would be harder to ensure that the data is accurate, relevant, timely, and complete. The problems associated with one data set may be multiplied across parallel data sets.
7. *Security*: Any data collected from the IOUs and stored pursuant to security protocols that are less rigorous than those utilized by the IOUs may be susceptible to loss, unauthorized access, destruction, modification, or unintended disclosure.
8. *Accountability and Auditing*: Mechanisms are already in place to enforce IOUs compliance with the FIPPs. It will be of utmost importance during the Working Groups to ensure that any other entity collecting and maintaining smart grid data be accountable for customer privacy in the same manner.

Both the FIPPs and SB 1476 were at the forefront when the Commission ultimately decided to adopt the Privacy Rules.

2. Privacy Rules, adopted in D. 11-07-056 (Attachment D)

Recognizing the need to more directly operationalize the FIPPs and the requirements of SB 1476 to protect consumer privacy in smart meter data,[19] the Commission adopted the Privacy Rules, which regulate the disclosure of energy usage data by IOUs. As noted above, last year the Privacy Rules were extended to cover gas utilizes, community choice aggregators, electric service providers, and other "load serving" entities.[20] The Privacy Rules determine the extent to which an IOU may disclose energy usage data to third parties, depending on the purpose for which the data will be used. It covers all energy usage data captured by smart meters that, "when associated with any information . . . can reasonably be used to identify an individual [utility customer] . . . ."[21] Data that cannot reasonably be re-identified are excluded from the Privacy Rules.[22]

---

[19] 2011 Decision, at 19–21.

[20] D. 12-08-045 (August 23, 2012).

[21] The exact language of the Privacy Rules reads:

> "Covered information" does not include usage information from which identifying information has been removed such that an individual, family, household or residence, or nonresidential customer cannot reasonably be identified or re-identified. Covered information, however, does not include information provided to the Commission pursuant to its oversight responsibilities.

The Privacy Rules categorize various potential uses into two categories. "Primary purposes" are uses of the data that directly serve utility operations, are specifically authorized by the utility company or the Commission in connection with an energy-related program, or are for services required by state or federal law. "Secondary purposes," cover all other uses. Each category comes with its own list of obligations and security protocols relating to data transfer. The Rules impose these obligations on both the IOU disclosing the data and the third party recipients of the data.[23]

a. Primary Purpose

Under the Privacy Rules, a covered entity may only disclose covered information without customer consent if the data will be used for a "primary purpose." The Privacy Rules identify four limited purposes that fit within this category:

> (1) [to] provide or bill for electrical power or gas,
>
> (2) [to] provide for system, grid, or operational needs,
>
> (3) [to] provide services as required by state or federal law or as specifically authorized by an order of the Commission, or
>
> (4) [to] plan, implement, or evaluate demand response, energy management, or energy efficiency programs under contract with an electrical corporation, under contract with the Commission, or as part of a Commission authorized program conducted by a governmental entity under the supervision of the Commission.[24]

Privacy Rules § 1(b). Further, for the purposes of "analysis, reporting or program management," disclosure of "aggregated usage data that is removed of all personally-identifiable information" is permissible, "provided that the release of that data does not disclose or reveal specific customer information because of the size of the group, rate classification, or nature of the information." Privacy Rules § 6(g).

[22] As explained in our accompanying memo titled *Technical Issues with Anonymization & Aggregation of Detailed Energy Usage Data as Methods for Protecting Customer Privacy*, which covers recent scientific advancements in re-identification, no level of basic anonymization and aggregation provides a guarantee against re-identification. The Commission should pursue more robust solutions.

[23] The Privacy Rules govern "covered entities," a category that includes:

> (1) [A]ny electrical corporation, or any third party that provides services to an electrical corporation under contract, (2) any third party who accesses, collects, stores, uses or discloses covered information pursuant to an order of the Commission, unless specifically exempted, who obtains this information from an electrical corporation, or (3) any third party, when authorized by the customer, that accesses, collects, stores, uses, or discloses covered information relating to 11 or more customers who obtains this information from an electrical corporation.

Privacy Rules § 1(a). The Commission's authority to create regulations binding on third parties derives from the language of SB 1476, which conferred upon the Commission "broad powers and a legislative mandate" to take regulatory action to protect consumer interests. 2011 Decision, at 33–35.

[24] Privacy Rules § 1(c).

Section 6(b) further clarifies which entities may access, collect, store and use covered information for primary purposes without customer consent:

- An electrical corporation
- A third party acting under contract with the Commission to provide energy efficiency or energy efficiency evaluation services authorized pursuant to an order or resolution of the Commission
- A governmental entity providing energy efficiency or energy efficiency evaluation services pursuant to an order or resolution of the Commission.[25]

According to the 2011 Decision, "[t]o the extent other governmental organizations, such as the California Energy Commission or local governments, may seek Covered Information in a manner not provided in these rules, the Commission will determine such access in the context of the program for which information is being sought absent specific Legislative direction."[26] Accordingly, where the Privacy Rules do not explicitly provide for a certain form of disclosure, the Commission will determine on a case-by-case basis whether the disclosure is appropriate, and whether it is permissible under relevant legislation, such as the IPA. Please see above for more information about the IPA.

Sections 6(c)(1)(a–b) provides additional insight as to what qualifies as a "primary purpose," and how disclosures must be carried out. Under these provisions, an IOU may share covered information with a third party without customer consent (a) if "explicitly ordered to do so by the Commission" or (b) if the disclosure serves "a primary purpose being carried out under contract with and on behalf of the electrical corporation disclosing the data."[27] These provisions indicate that the Commission intended for the "primary purpose" category to cover a fairly narrow selection of disclosure scenarios, largely directed to IOU operations (such as billing, maintenance, and the like by contractors), along with the noted services, when under direct Commission oversight.

"Primary purpose" disclosures create a chain of obligations that carry down to subsequent custodians of "covered information." When disclosure occurs for a "primary purpose," the covered entity disclosing the data "shall, by contract, require the third party to agree to access, collect, store, use, and disclose the covered information under policies, practices and notification requirements no less protective than those under which the covered entity itself operates as

[25] Privacy Rules § 6(b).
[26] *See* 2011 Decision at 47-48.
[27] Privacy Rules §§ 6(c)(1)(a–b).

required under this Rule, unless otherwise directed by the Commission." Thus, a "primary purpose" recipient of covered information must employ at least the same privacy and security measures as those implemented within the IOU from which it collected the data. The Privacy Rules attach to all data that originates with the IOUs, regardless as to whom ultimately takes possession of it.[28]

b. Secondary Purpose

Any purpose that does not fall within one of the above categories is considered a "secondary purpose" under the Privacy Rules.[29] IOUs are prohibited from disclosing covered information for any secondary purpose without the "prior, express, written authorization" of each utility customer represented in the data.

Three limited exceptions to this requirement exist. A covered entity may only disclose smart grid data without customer consent in the following situations: (1) disclosure pursuant to a certain types of legal process (such as a warrant or court order); (2) disclosure in "situations of imminent threat to life or property; and (3) disclosure "authorized by the Commission pursuant to its jurisdiction and control."[30] Again, without an authorization order from the Commission, third parties not working on behalf of the utility company likely cannot obtain covered information without the prior, express, written authorization from utility customers.

c. Data Minimization Requirements

Under Section 5(c), covered entities must limit the disclosure of smart grid data to only that which is "reasonably necessary or as authorized by the Commission" to carry out the specific purpose permitted under the Privacy Rules. For data uses constituting "secondary purposes," this means that the covered entity may not disclose more information than is

---

[28] Privacy Rules § 6(c)(1). Rule 6(c)(2) reinforces the recursive nature of the Privacy Rules:

> Any entity that receives covered information derived initially from a covered entity may disclose such covered information to another entity without customer consent for a primary purpose, provided that the entity disclosing the covered information shall, by contract, require the entity receiving the covered information to use the covered information only for such primary purpose and to agree to store, use, and disclose the covered information under policies, practices and notification requirements no less protective than those under which the covered entity from which the covered information was initially derived operates as required by this rule, unless otherwise directed by the Commission.

Privacy Rules § 6(c)(2).

[29] Privacy Rules § 1(e).

[30] Privacy Rules §§ 6(d)(1–3).

reasonably necessary to carry out the specific purpose authorized by the customer in writing. As noted above, data minimization requires entities to consider, in advance of disclosure, what data is reasonably necessary for the agreed-upon purpose before disclosing the data.

d. Data Security and Breaches

Section 8 of the Privacy Rule establishes the minimum security requirements that covered entities must employ when in possession of covered information. "Covered entities shall implement reasonable administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure."[31] Furthermore, when a breach has been detected, a covered third party must notify the disclosing IOU within one week, and the utility must notify the Commission of all breaches affecting one thousand or more customers.[32] Utility companies are additionally obligated to file an annual report at the end of the each calendar year, chronicling all security breaches affecting covered information that year.

e. Enforcement and Recourse for Privacy Rule Violations

If a recipient party fails to comply with its contractual obligations to handle the covered information in a manner "no less protective" than those under which the originating entity operates—a "material breach" under the Privacy Rule—"the disclosing entity shall promptly cease disclosing covered information to such third party."[33]

CONCLUSION

The laws and regulations described above each bear heavily on the data sharing scenarios contemplated within this proceeding. As such, it will be important for participants to enter the Working Group discussions with a firm understanding of their relevant provisions, with the Privacy Rules front and center.

Among the California state Constitution, the IPA, the FIPPs, SB 1476, and the Privacy Rules, utility customers receive legal protections for the privacy of their energy usage data.

[31] Privacy Rules § 8(a).
[32] Privacy Rules § 8(b). The Commission may also request that the utility company provide notification of any other breach for which notification is not already compulsory.
[33] Privacy Rules § 6(c)(3).

These protections, in various ways, bind the IOUs, the Commission, and other state agencies handling smart meter data, as well as third parties who obtain energy usage data from the utilities. At this stage of the proceeding, keeping these laws and regulations in mind will better position the Working Groups to devise solutions that are appropriately tailored to each disclosure scenario and are consistent with applicable law.

Respectfully submitted this April 1, 2013 at San Francisco, California.

/s/ Jennifer Urban

JENNIFER URBAN, Attorney
Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7338
Attorney for ELECTRONIC FRONTIER FOUNDATION

/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