Future of Privacy Summary of
California Public Utilities Commission Proposed Decision
on Smart Grid Privacy and Security

May 9, 2011

On May 6th, the California Public Utilities Commission (CPUC) issued a proposed decision by CPUC President Peevey addressing smart grid privacy and security. The CPUC proposed decision presents the most significant step yet in the U.S. towards a comprehensive set of smart grid privacy rules. The CPUC is accepting comments regarding its proposed rules until May 26, 2011.

The proposed decision develops a regulatory framework that is wide-ranging in reach. It would apply privacy and security rules to customers of California's three investor-owned electric utilities offering or proposing to install smart meters, Pacific Gas and Electric Company (PG&E), Southern California Edison Company (SCE), and San Diego Gas & Electric Company (SDG&E). It would extend the proposed rules to companies that contract with these utilities. Most notably, the proposed rules would also apply, by utility tariffs, to certain other third party companies that are not in contractual privity with a utility.

Specifically, a third party would have to comply with the PUC rules when it obtains access to customer's usage data via Home Area Netwok (HAN)-enabled devices that are "locked" to automatically transfer usage data to the third party. In addition, the proposed rules would require utilities to provide third parties with access to usage data that customers authorize if the third parties comply with the privacy and security rules. The PUC rejected suggestions that third parties should be required to register for certification to offer services that require access to customer energy consumption data.

The following summarizes some of the key aspects of the proposed decision.

PUC's Assertion of Jurisdiction Over Third Parties

In assessing its jurisdiction, the Commission examined its general regulatory authority as well SB 1476, the smart grid privacy law that took effect January 1, 2011. The PUC focused

especially on the provisions of SB 1476 that address requirements utilities must impose on third parties with whom they contract with either to perform utility functions or to enable customer monitoring of energy usage information. *See* Cal. Pub. Util. Code § 8380. Based on those provisions, the PUC concluded that it had authority to enact rules relating to third parties that contract with utilities.

The PUC also considered its jurisdiction over third parties that obtain energy consumption data through channels independent of the utility, either from a HAN device or from the utility customer. The PUC concluded it has jurisdiction to ensure compliance with its privacy and data security rules for some of these third parties. The PUC noted that a non-utility HAN-enabled device must already be authorized through registration with the utility to allow the direct transfer of data from the Smart Meter to the third party. The PUC concluded that for HAN-enabled devices "locked" (i.e., designated for that third party alone) for automatic transfers of data to the third party, utility tariffs should govern these third parties' activities. Specifically, utility tariffs should require as a condition of registering the device with the Smart Meter, that the third party show that it has consumer consent for the proposed uses of data and that it is in compliance with PUC requirements for protecting consumer data.

The PUC declined to assert authority over other third parties offering HAN-enabled devices that do not automatically transfer information to a third party. Instead, under the PUC's framework, it would require utilities through tariffs, to provide consumers with information about the potential uses and abuses that arise from sharing energy usage data with third parties. The PUC would also not attempt to regulate consumers and what they choose to do with their own usage data.

With the exception of consumer consent requirements, the PUC would exempt fully from the proposed rules third parties that obtain information regarding ten or fewer households. The PUC proposes this exemption to avoid regulating situations where a friend or family member has access to usage information in the course of caring for others.

Summary of Proposed Rules

The PUC's proposed rules draw from months of hearings and comments filed in its consideration of smart grid privacy and from the intervening passage of SB 1476 on September 29, 2010. As a result of those proceedings, the PUC expressly embraces and follows an approach to protect consumer privacy based on Fair Information Practice (FIP) principles: (1) Transparency, (2) Individual Participation, (3) Purpose Specification, (4) Data Minimization, (5) Use Limitation, (6) Data Quality, (7) Security, and (8) Accountability and Auditing. The PUC's proposed rules draw heavily from suggested rules presented to the PUC last year by the Center for Democracy and Technology (CDT) and the Electronic Frontier Foundation (EFF), with some modifications.

1. Definitions

There are 5 primary defined terms used throughout the proposed rules whose meaning is important to the rules' application: (1) Covered Entity; (2) Customer; (3) Covered Information; (4) Primary Purposes; and (5) Secondary Purposes.

Covered Entity: A "covered entity" is "(1) any electrical corporation [currently just PG&E, SCE, and SDG&E] or any third party that collects, stores, uses, or discloses covered information relating to 11 or more customers who obtains this information from an electrical corporation or through the registration of a locked device that transfers information to that third party."

Customer: A "customer" is "any entity receiving retail generation, distribution or transmission service from an electrical corporation."

Covered Information: "Covered information" is "any usage information obtained through the use of the capabilities of Advanced Metering Infrastructure when associated with any information that can reasonably be used to identify a customer." However, "covered information does not include usage information from which identifying information has been removed such that a customer cannot reasonably be identified or re-identified."

Primary Purposes: "Primary Purposes" relating to "the collection, storage, use or disclosure of covered information" include (1) providing or billing for electrical power, (2) fulfilling other operational needs of the electrical system or grid, (3) providing services as required by law or order of the PUC, or (4) planning, implementing or evaluating demand response, energy management, or energy efficiency programs operated by, or on behalf of and under contract with, an electrical corporation.

Secondary Purposes: Any purpose that is not a primary purpose.

2. Transparency (Notice)

The proposed rule contemplates both a notice and a privacy policy. The proposed rules would require that covered entities "provide customers with meaningful, clear, accurate, specific, and comprehensive notice regarding the collection, storage, use, and disclosure of covered information." Covered entities must provide the notice when confirming a new customer account and at least twice a year. The notice must be written or electronic and it must advise customers how they may obtain a copy of the covered entity's privacy policy. Covered entities must also post or provide a link to the notice and privacy policy on the home page of their website and include a link to the notice and privacy policy in all electronic communications to customers.

The notice must make clear it is a privacy notice and shall "easily understandable" and "no longer than necessary to convey the requisite information." Both the notice and privacy policy must identify the covered entity, include the effective data, address how customers will be

advised of alterations, and provide contact information for an official to answer questions or complaints.

3. Purpose Specification

The proposed purpose specifications would require that the notice discussed above "explicitly describe each category of covered information collected, used, stored or disclosed by the covered entity" and the purposes for doing so. In addition, as proposed, the notice must also describe:

- Each category of personal information the covered entity discloses to third parties, the purposes for such disclosure and the "number and categories of third parties to which it is disclosed."
- Retention timeframes.
- How customers can access and address disputes about their covered information
- How customers can limit covered information collection, use, storage or disclosure and the consequences to customers of doing so.

4. Individual Participation (Access and Control)

The proposed rule would require that customers have access to their covered information and control over its use and disclosure. Covered entities must provide access to customers in an "easily readable format" at least as detailed as what covered entities provide third parties. Customers must have "convenient mechanisms" to approve and revoke approval for secondary uses of their covered information. Customers must also be able to correct and amend their information.

The proposal would strictly limit disclosure to third parties. Except as otherwise permitted by the proposed rules or other laws, a covered entity would be prohibited from disclosing covered information except pursuant to a warrant or court order, with the express consent of the customer, or to emergency responders in situations involving imminent threat to life or property. Real-time information access requests would be governed by state and federal wiretap laws. If a covered entity receives a subpoena, it would be required to notify the customer in writing and provide the customer with 7 days to appear and contest the information sought, subject to any legal prohibitions on advance disclosure. The proposed rules do not prevent a covered entity from disclosing customer contact information pursuant to a subpoena. Covered entities would be required, upon request, to provide reports to the PUC regarding requests made pursuant to legal process.

5. Data Minimization

Covered entities would only be allowed to collect, use, store, retain, and disclose covered information as is "reasonably necessary" or "authorized by the Commission" to accomplish a specific primary purpose or a secondary purpose authorized by customers.

6. Use and Disclosure Limitation

Under the proposed rules, electrical corporations may collect, store, and use customer information without customer consent if for primary purposes. Other covered entities generally must have prior customer consent.

The proposed rules include a service provider exception to prior customer consent for all covered entities. Specifically, any covered entity would be permitted to disclose customer information to a third party without customer consent:

- pursuant to PUC order, or
- for a primary purpose performed under contract with and on behalf of the disclosing entity, if:
    - the contract with the third party obligates it to treat covered information "under policies, practices and notification requirements" at least as stringent as those the covered entity is required to operate under the proposed rules, and
    - where the information is disclosed to third party for "demand response, energy management or energy efficiency purposes, the disclosing entity affords customers an opt-out option consistent with program terms and conditions.

Third party sharing with sub-contractors is permitted under similar restrictions. Any covered entity that discovers a pattern or practice of third parties violating these provisions would be required to stop disclosing covered information to those parties.

Covered entities would be required to obtain customers' "prior, express, written authorization" for using or disclosing covered information for secondary purposes, except as permitted in section 4 above. Residential customers would have the right to revoke authorization at any time through the same mechanism used to provide consent and covered entities shall notify customers at least annually of their right to revoke.

The proposed rules would not restrict covered entities from sharing aggregated de-identified data for "analysis, reporting or program management." Such data cannot reveal specific customer information.

7. Data Quality and Integrity

Covered entities would be obligated to ensure data is reasonably complete and accurate or otherwise handled consistent with applicable rules and tariffs.

8. Data Security

The proposed data security rule would obligate covered entities to implement reasonable administrative, technical and physical safeguards to protect covered information. In addition, the proposed rules address data breaches. Covered third parties must notify the disclosing party within one week of detecting a breach. A covered electrical corporation must notify the PUC of any breach affecting 1,000 or more customers within two weeks of detecting its own breach or within one week of notification from a third party. Beginning in 2010, covered electrical corporations must provide an annual report to the PUC notifying it of all security breaches. The proposed rules do not define a security breach. As to individual notice, the PUC stated it would expect covered entities to comply with federal and state breach notification laws.

9. Accountability and Auditing

Under this proposed rule, the PUC imposes separate independent data security and privacy audit and reporting requirements on electrical corporations. However, in addition, all covered entities would be required, upon PUC request or audit, to provide:

- the privacy notices given to customers,
- internal privacy and data security policies,
- the identity of third parties to whom covered information is disclosed, and
- copies of secondary uses authorization forms.

Covered entities would also be required to develop a process to address customer complaints. The proposed rules also call for covered entities to provide employee and contractor training.

Other Issued Addressed by the PUC

The PUC also addressed the obligations of PG&E, SCE, and SDG&E to provide access to customer energy consumption data to third parties. Regarding data provided via the backhaul (i.e., an Internet connection with the utility), the PUC noted that SDG&E already enables third parties, such as Google through its PowerMeter, to make consumption information available to its customers. The PUC concluded that "[t]here is no reason why SCE and PG&E should not provide access to authorized parties to consumer usage data available through the backhaul as SDG&E already does." It believes requiring access is reasonable and in the public interest. Accordingly, the PUC proposes that PG&E and SCE make appropriate filings with tariffs enabling third party access to usage data when authorized by the consumer and where the third parties agree to the privacy and data security protections adopted in the proceeding.

Regarding third party access to more granular consumption data for customers through devices that connect directly to the smart meter, such as HAN devices that "lock" and automatically transmit meter data to the third party, the PUC believes the considerations are the same. Noting that the development of communication standard SEP 2.0 has been delayed, the PUC proposed that PG&E, SCE and SDG&E develop pilot projects for HAN enabled devices to connect to smart meters. The goal would be to determine the best methods to afford customers with direct access to disaggregated data available in smart meters and to encourage these companies to work toward a common interface for third party and customer devices.

The PUC also addressed PG&E, SCE and SDG&E's provisioning of pricing information to customers. The PUC proposes that the companies should make approximate price information available to customers online, available at least one day later on a daily basis and updated in hourly or 15 minute increments. This should include bill-to-date, bill forecast data, projected month-end tiered rate, and notices to customers when they cross rate tiers. The PUC also called for the companies to work together to provide consumers with wholesale price information. The PUC declined to propose an order to make near-real time price information available because of the complexity of current tariff schedules. The PUC expects to revisit this issue in the context of HAN and HAN-enabled devices.

* * *

The proposed rules are significant in that they would become the first comprehensive set of rules in the United States. The proposed rules state that further study is not required and that the time for rules is ripe. As noted at the outset, the PUC is accepting comments on the proposed rules until May 26, 2011. Reply comments will be accepted 5 days after that.