



**BEFORE THE PUBLIC UTILITIES COMMISSION  
OF THE STATE OF CALIFORNIA**

**FILED**

11-08-10  
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.

R.08-12-009

**REPLY COMMENTS OF THE CONSUMER FEDERATION OF CALIFORNIA ON  
POLICIES AND PROCEDURES TO PROTECT THE PRIVACY AND SECURITY OF  
CUSTOMER INFORMATION AND PRICING INFORMATION COMMUNICATED TO  
CUSTOMERS**

Alexis K. Wodtke  
Nicole A. Blake

CONSUMER FEDERATION OF CALIFORNIA  
520 S. El Camino Real, Suite 340  
San Mateo, CA 94402  
Phone: (650) 375-7847

## TABLE OF CONTENTS

I.	<b>THE IMPORTANCE OF PROTECTING PRIVATE INFORMATION</b>	3
II	<b>THE TECHNOLOGY</b>	3
III.	<b>THE RIGHT TO PRIVACY</b>	5
A.	<u>Informed Consent to 3<sup>rd</sup> Parties' Use of Energy Consumption Data</u>	6
B.	<u>Controlling Release of Energy Usage Data</u>	8
1.	<i>SB 1476</i>	8
2.	<i>Relevant California Privacy Laws</i>	9
a.	<u>Defining Personal Information</u>	9
b.	<u>The Substance of Consent</u>	11
c.	<u>Disposal of Records</u>	12
d.	<u>Notification of Breach</u>	12
e.	<u>Liability for Breach</u>	12
3.	<i>Commission Decisions</i>	12
a.	<u>Customer Consent Required</u>	13
b.	<u>Customer Information Used by Contractors</u>	14
IV.	<b>PRACTICES OF CALIFORNIA UTILITIES</b>	14
A.	<u>There Is A Question About Whether The Utility Will Retain The Role Of Caretaker For Customer Usage Data</u>	15
B.	<u>Liability for Information Leaks</u>	16
C.	<u>Protocols and The Cost of Gathering Data?</u>	18
1.	<i>Open ADE or Smart Energy Standards</i>	18
2.	<i>Security Measures, Now and in the Future</i>	20
V.	<b><u>Reply Comments for Providing Pricing Information</u></b>	31

A. Background ..... 31

B. Summary of Viewpoints regarding pricing information ..... 31

C. Utilities’ Pricing Proposals ..... 32

**I. THE IMPORTANCE OF PROTECTING PRIVATE INFORMATION**

Two conflicting policies must be reconciled when the Commission determines what access to meter data will be allowed to third parties. The first, and most important, is keeping private the personal information of the customer. The second is to encourage innovation by allowing third parties to use energy usage data to inform the state’s energy efficiency efforts. As stated by NTIA, “Here’s the crux of the issue: On one hand it’s clear that intensive use of personal information can fuel the development of new Internet products and services. On the other hand, we know that if consumers do not trust that information about them will be kept secure and used appropriately, they’ll be reluctant to use new services.”<sup>1</sup>

**II THE TECHNOLOGY.**

Smart Meters are radio transmitters, sending radio frequency microwave radiation (RF) signals from both electric and gas meters. The electric meter has two transmitters. One RF signal is sent directly into your home (or business), and the other to a neighborhood data collector, which could be located on a lamppost, telephone pole, building or a home. Homes will also be used as repeaters for neighborhood RF signals.<sup>2</sup> According to EMF Safety Network, “A professional EMF electrician has measured a Smart Meter and found they emit RF every 45 seconds. Another professional expert has measured one or more a minute, on a random basis.

Inside the home, “a Home Area Network, which includes an RF interior display unit,” will be installed and appliances will be retrofitted with antennas, or new “smart” appliances will be purchased. ... Installing these interior devices will allow the Utility

---

<sup>1</sup> National Telecommunications and Information Administration (NTIA): A. Gomez “Remarks for the Safe Internet Alliance Workshop on *Safer by Design: Policies and Principles*. (Sept. 29, 2010) [http://www.ntia.doc.gov/presentations/2010/safeinternetalliance\\_09292010.html](http://www.ntia.doc.gov/presentations/2010/safeinternetalliance_09292010.html)

<sup>2</sup> Earthcalm.com, “Are Smart Meters Smart?” <http://earthcalm.com/2010/are-smart-meters-smart/>

company to further control the electric grid, by turning off certain appliances during peak use time, if needed.”<sup>3</sup>

“This HAN feature is built into the ZigBee chip sets. When the new ZigBee 2.0 Standard is approved, your meter can become just another node on your WiFi network. This will enable realtime monitoring of usage on multiple devices in the home, from your laptop, PDA, cellphone, or wireless integrated TV set, or dedicated display. . You will be able to turn off the TV using a cellphone from work, if you left the house with it on.”<sup>4</sup>

San Diego Gas & Electric (SDG&E) “is providing customer hourly interval electric usage data via Google’s Power Meter (GPM). A customer must provide their explicit consent (via written or electronic authorization) before such a transfer of their energy usage data can be initiated. . . . Only customer specific electric usage data is transferred and no personal customer information is transferred to the customer’s designated third party.”<sup>5</sup>

Now, Google and Energy Inc. have formed a partnership allowing bypass of the smart meter. “Google's PowerMeter and Energy Inc.'s TED 5000 (“The Energy Detective”) work together without the need for a smart meter. Homeowners can monitor their energy use from a Web browser or smart phone equipped with iGoogle. The information provided includes real-time energy use and approximate cost, trends and comparisons to previous use”<sup>6</sup> The Google/TED system bypasses the utility’s network and consequently a utility is not in a position to control the gathering of data.

There are other devices which can be used to read the meter from the customer’s side. Where a utility provides pulse output from their meter, devices like Siemens’ and Energy Tracking’s ‘web enabled pulse logger’ can be used to acquire consumption data in real-time via email, ftp, or direct access. Black & Decker, Blue Line Innovations, P3 International and others make ‘power monitors’ a wireless outdoor monitor which you mount on your electric meter; it monitors your electric usage and

---

<sup>3</sup> *Id.*

<sup>4</sup> R. Steele, *Oh my, PG&E Smart Meters are coming to our house* (May 22, 2010)

<sup>5</sup> SDG&E Pre-hearing Conf. Statement (Aug. 13, 2010) at 6-7.

<sup>6</sup> VENTUREBEAT.COM, *Google Lands Energy Device Partner, Doesn’t Have To Wait For Smart Meters* (Oct. 5, 2009). .” “The system includes a transmission unit that connects directly into a building’s circuit breakers and a compact screen display that plugs into any electrical unit. This component tells you how many kilowatts you are using and how much your energy consumption at any given moment is costing per hour, as well as how much money you’ve spent on energy in the month to date.”

sends to your home network real time readings in both dollars and KWH from your electric meter.<sup>7</sup> Leviton, GE, Trane, and Honeywell all have energy management devices, as well. Each of these developers would, presumably, be interested in buying personal information from a utility.

The recent release of National Institute of Standards and Technology (NIST) Report on Cybersecurity emphasizes the importance of developing methods to secure data usage systems as soon as possible.

While integrating information technologies is essential to building the Smart Grid and realizing its benefits, the same networked technologies add complexity and also introduce new interdependencies and vulnerabilities. Approaches to secure these technologies and to protect privacy must be designed and implemented early in the transition to the Smart Grid.<sup>8</sup>

### III. THE RIGHT TO PRIVACY.

California's Constitution guarantees to the people a right of privacy:

All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.<sup>9</sup>

The NIST report describes the generally recognized right to keep personal information private: “[T]he right to control when, where, how, to whom, and to what extent an individual shares their own personal information,” defined as “any information relating to an individual, who can be identified, directly or indirectly, by that information.”<sup>10</sup> The Privacy Rights Clearinghouse offers a similar description: “Your personal information is more than your name, address and Social Security number. It includes your shopping habits, driving record, medical diagnoses, work history, credit score and much more. ... The *right to privacy* refers to having control over this personal information. It is the ability

---

<sup>7</sup> ProTool Reviews.com, <http://www.protoolreviews.com/reviews/electrical/misc/black-decker-em100b>

<sup>8</sup> NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), Interagency Report 7628 (hereafter NIST Report 7628), vol. 2, p.2. (August 2010)

<sup>9</sup> Cal. Const. Art. 1, sec. 1.

<sup>10</sup> NIST There can be no doubt that customers own the energy usage data kept by a utility. The data would not exist but for the customer. The data is personal information gathered, but not owned, by the utility for operating and billing purposes only. The data has not been available to third parties in the past, with a few exceptions.

to limit who has this information, how this information is kept and what can be done with it.”<sup>11</sup>

A. Informed Consent to 3<sup>rd</sup> Parties’ Use of Energy Consumption Data.

Energy usage data is quite valuable. It can be sold or made available to third-party marketers, law enforcement agencies investigating possible criminal acts, insurance companies seeking to identify unhealthy behaviors in order to adjust rates, criminals attempting to perpetrate illegal acts, researchers looking to create new energy-related studies, and competing businesses or manufacturers wishing to access trade secrets of competitors.”<sup>12</sup> The unauthorized acquisition of energy usage data has attracted much attention.

For example, Google has been in trouble with the FTC, Canada, Australia, the UK, the Czech Republic, Spain, Germany, Hong Kong and others for ‘inadvertently’ gathering personal data during drives through various neighborhoods to supplement its maps:

Google said that its cars taking pictures of buildings along city streets, which had also checked for Wi-Fi hotspots, had collected even more information about Internet users than it had first thought last May. That information included passwords, e-mail messages and Web addresses carried on unencrypted Wi-Fi networks, Google said. Google stopped driving Street View cars in May and restarted in the summer, but without collecting Wi-Fi data.<sup>13</sup>

Tendril urges the Commission to simplify the process whereby customers give consent to the release of their energy usage data, and make that consent permanent unless rescinded by the customer. Customers deserve the opposite approach. They should be fully informed of the rights they are conceding to the third party before granting consent, and the consent should expire at reasonable intervals so that customers have an opportunity to withdraw that consent. CFC supports DRA and TURN’s proposal to require that a two-year sunset provision be included in any contract conveying customer consent to the release of personal data.

---

<sup>11</sup> Privacy Rights Clearinghouse, *Why Privacy?*

<sup>12</sup> Comments of the National Association Of State Utility Consumer Advocates (NASUCA) (July 12, 2010) in response to a FERC Request for Information (RFI) *Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy*. See 75 Fed. Reg. 26203 (May 11, 2010)

<sup>13</sup> N.Y. Times, *A Reassured F.T.C. Ends Google Street View Inquiry* (Oct. 27, 2010)

Customer consent must mean something more than having a piece of paper put down in front of you for your signature. The NIST suggests that “[m]ost consumers probably do not understand their privacy exposures or their options for mitigating those exposures within the Smart Grid.”<sup>14</sup> They need to know these things.

In order to control the spread of their energy usage data beyond the utility, customers must be given an opportunity to specify how it will be used, if at all. CDT has proposed rules which are designed to fully inform the customer of the justification for gathering their usage data, the uses that may be made of the data, and their right to give or deny consent to its release to a third party. These rules offer a platform on which to build protections for customers’ private information.

In order to assure that the customer gives informed consent for the release of personal data, customer education is required.<sup>15</sup> The utility or a third party must explain:

- the deployment of smart meters,
- the enhanced communications abilities,
- the scope of information to be gathered,
- the possible additional uses to which that data may be employed,
- the ability of the customer to choose to participate in the gathering of the data and its sharing,
- the right of the customer to elect not to participate,
- the ability to revoke any prior election to participate,
- the telephone number of the customer service representative to whom calls about concerns or problems may be directed,
- the telephone numbers of regulatory and advocacy entities in the jurisdiction to whom a customer may turn for additional assistance.”<sup>16</sup>

---

<sup>14</sup> NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), Interagency Report 7628 (hereafter NIST Report 7628), vol. 2, p.2. (August 2010)

<sup>15</sup> Strikingly, the Edison Electric Institute (EEI) made a similar recommendation in a FERC proceeding. Comments of EEI (July 12, 2010) in response to a FERC Request for Information (RFI) *Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy*, p. 10.. See 75 Fed. Reg. 26203 (May 11, 2010)

“The granularity, or depth and breadth of detail, captured in the information collected and the interconnections created by the Smart Grid are factors that contribute most to these new privacy concerns.”<sup>17</sup>

B. Controlling Release of Energy Usage Data.

1. *SB 1476*

The passage of SB 1476 established a general standard for the protection of customer data, although there are holes a truck can drive through in the statute.

Additional protection for customer data is needed.

In general, the legislature has established the following standards:

- An energy utility shall not sell a customer’s electrical or gas consumption data or any other personally identifiable information for any purpose. (Section 8380(b)(2))
- An energy utility shall use reasonable security procedures and practices to protect a customer’s unencrypted electrical or gas consumption data from unauthorized access, destruction, use, modification, or disclosure.
- Neither the energy utility nor its contractors shall bribe the customer (through an incentive or discount) to allow access to the customer’s data, unless the customer agrees.<sup>18</sup> Given the possibility of reduced rates, why wouldn’t a customer agree?
- When a utility contracts with a 3<sup>rd</sup> party to enable a customer to monitor energy usage data, that contract must prominently disclose the fact that the third party may use the data for a secondary commercial purpose, as well. This section does not require that the customer be made aware of the third party’s plans, nor does it require customer consent.
- Where an energy utility uses an advanced metering infrastructure where the customer can access his or her data, the customer may not be coerced into allowing the utility or a third party access to the customer’s data as a condition for that access.

Notwithstanding the foregoing protections, SB 1476 allows an energy utility, after January 1, 2011, to disclose the customer’s energy usage data to a third party “for

---

<sup>16</sup> Comments of the National Association Of State Utility Consumer Advocates (NASUCA) (July 12, 2010) in response to a FERC Request for Information (RFI) *Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy*. See 75 Fed. Reg. 26203 (May 11, 2010)

<sup>17</sup> NIST Report 7628, at 4.

<sup>18</sup> Customer consent, under these circumstances, would violate Pub. Util. Code sec. 453.

system, grid, or operational needs, or the implementation of demand response, energy management or energy efficiency programs,” without customer consent, *if* the energy utility enters into a contract which

- requires the third party to adopt and use “reasonable security procedures and practices appropriate to the nature of the information, to protect the customer data from unauthorized access, destruction, use, modification or disclosure (Section (e)(2))
- prohibits the use of the data for commercial purposes unless related to the primary purpose of the contract, in which case the customer must consent.

Given this degree of protection (or lack thereof), it is imperative that the utility be made responsible for enforcement of the contract under which energy usage data is released, and that the utility remain liable, either jointly with the third party or as an indemnitor, for any breaches of that contract by the third party. Holding the utility liable will provide the necessary incentive for the utility to actively monitor the third party’s actions, particularly in cases where customer consent is not required. (*See discussion, below*). Requiring a utility to record liability payments ‘below the line’ would add further incentives to supervise third parties’ use of customer information. This is a fair resolution since the utility is responsible for releasing the energy usage data originally and for drafting the contract under which uses of that data are specified.

## 2. *Relevant California Privacy Laws*

We may also look at other laws, rules and decisions to determine what privacy protections there are or should be for energy usage data. Statutes referenced by Pacific Gas & Electric Company (PG&E) provide a useful indication of the privacy expectations of the legislature.

### a. Defining Personal Information**Error! Bookmark not defined.**

Pub. Util. Code sections 394.4 and 2891, Bus. & Profession Code section 22577, and Civil Code section 1798.81.5, each require that customer information be maintained securely,. They are useful in defining what customer information should be kept confidential.

Civil Code section 1798.81.5 applies to any 'business', defined broadly, but not to a business that is "regulated by state or federal law providing greater protection to personal information than that provided by this section." The protection required by the statute is to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."<sup>19</sup>

Section 1798.81.5 describes "personal information" as including but not limited to, "personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates." Personal information is more specifically defined in section 1798.80, to include:

"Personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

22577. For the purposes of this chapter, the following definitions apply:

(a) The term "personally identifiable information" means individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:

- (1) A first and last name.
- (2) A home or other physical address, including street name and name of a city or town.
- (3) An e-mail address.
- (4) A telephone number.
- (5) A social security number.

---

<sup>19</sup> The statute also requires that any business that "discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(6) Any other identifier that permits the physical or online contacting of a specific individual.

The definition offered by SDG&E addresses only customer usage: “The electric or gas energy that the customer consumed as measured by the metering device. ... Usage data includes information necessary to compute the customer bill (often referred to as customer specific billing determinants).”<sup>20</sup> It does not address other personal information which SDG&E describes as follows:

PII includes any personal identification such as name, service/billing address, phone number, email address, and social security number. It also includes consumption information such as usage amounts and patterns and credit history such as records of customers’ payment histories.<sup>21</sup>

Section 394.4(a) applies to energy service providers, and requires that certain customer information be kept confidential unless the customer consents to its release. Information protected by the statute is “customer specific billing, credit, or usage information,” unless the data is sufficiently generic that it does not reveal customer specific information.

Section 2891 applies to telephone companies and prohibits the company from disclosing, without customer consent, a subscriber’s personal calling patterns (similar to energy usage data), the residential subscriber's credit or other personal financial information, the services which the residential subscriber purchases, demographic information about individual residential subscribers.

b. The Substance of Consent

Section 2891.1 also specifies the nature of written consent to be given before information is released. The express consent must be either “a separate document that is signed and dated by the subscriber, and that is not attached to any other document,” or an “affirmative response made on a separate field on an Internet Web site where there is no default,” to be followed by “a confirmation notice to the subscriber's electronic mail address, or to a subscriber's postal mail address. The express consent “shall be unambiguous, legible, and conspicuously disclose” the use which will be made

---

<sup>20</sup> SDG&E Response Comments (Oct. 15, 2010) at 4.

<sup>21</sup> SDG&E Response Comments at 7.

of the customer information. And, finally, section 2891(c) ensures the customer a right to rescind his or her consent to the release of personal information by notice, which must be honored within the following 30 days.

c. Disposal of Records.

Civil Code section 1798.81 requires a business to “take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.”

d. Notification of Breach

Section 1798.82 requires a business to “disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay.” The statute defines what constitutes a breach of security as “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.”

e. Liability for Breach

Section 1798.83 imposes liability on a business for injuries to people whose personal information has been released. An injured party may bring a civil action for damages, including attorney fees, and may also recover a civil penalty of up to \$500 per violation of Section 1798.83 and, if willful, intentional, or reckless, up to \$3,000 per violation.

3. *Commission Decisions*

Commission decisions cited by PG&E provide a record of the Commission’s protection of private, personal information. In D.90-12-121, the Commission found “[t]he present stated practice at all respondent energy utilities is not to make commercial use of customer information. All utilities expressed no desire or intention to do so. ... CLECA

and CMA both expressed objections to release of information concerning customer usage, in particular.<sup>22</sup>

a. Customer Consent Required.

When direct access began, the Commission considered the question of how to level the playing field for energy service providers competing against utilities. The Commission ordered in D.97-05-040 that “customer-specific information necessary for the distribution functions of the utility be made available to all competitors, on terms that are fair to all competitors.”<sup>23</sup> The details concerning what information would be made available to ESPs were discussed in D.97-10-031.<sup>24</sup> In both instances, however, the Commission held that no information about a particular customer would be released without customer consent. In D.98-03-073, the Commission restated the basic policy it had established when adopting rules for affiliate relationships: “Disclosure of utility and utility customer information should be prohibited, with the exception of customer-specific information where the customer has consented to disclosure.”<sup>25</sup>

More than ten years later, the Commission reaffirmed that policy. In D.09-09-047, the Commission was asked by the Local Government Sustainable Energy Coalition (LGSEC) to eliminate the prior consent requirement for data requested by local governments. Two types of data were needed, local governments argued, “facility specific data to benchmark their own facilities” and “data aggregated by sector (residential, commercial, and industrial sectors, etc.) to create community inventories, or profiles” for climate action plans and the like.<sup>26</sup> The utilities were willing to supply aggregated data, but not private customer data related to specific buildings, without prior customer consent. The Commission stated that it was “sympathetic to the requests of local governments but mindful of the need to maintain the privacy of our ratepayers and legal restrictions on the dissemination of consumer information.”<sup>27</sup> It pointed out that under Tariff Rule 22, customer consent requirements for usage data requested by direct access customers “had been in place for ten years and, to our

---

<sup>22</sup> 1990 Cal. PUC LEXIS 1408, \*16-17; 39 CPUC2d 173 (Dec. 27, 1990)

<sup>23</sup> D.97-05-040, 1997 Cal. PUC LEXIS 341, \*130-31; 72 CPUC2d 441 (May 6, 1997)

<sup>24</sup> *Id.* at 96.

<sup>25</sup> 1998 Cal. PUC LEXIS 1, \*15; 79 CPUC2d 343; citing D.97-12-088

<sup>26</sup> D.09-09-047 at 252 (2009)

<sup>27</sup> D.09-09-047 at 253.

knowledge, this requirement has worked.”<sup>28</sup> It asked the utilities to “facilitate the transfer of usage data for private buildings authorized by written paper or electronic customer consent.”<sup>29</sup>

b. Customer Information Used by Contractors

In D.00-07-020, the Commission considered whether outsourcing jobs entailed in managing the Low Income Energy Efficiency (LIEE) program made sense. One potential obstacle considered was the release of customers’ personal information to contractors. The Commission described the conditions under which such a release might be permitted:

This information should be provided to the contractor, *at cost*, provided that: (1) the contractor has documented its need for such records based on the specifics of its program implementation or marketing plan, and (2) appropriate security arrangements that will protect the confidentiality of these records have been made. The utilities shall negotiate with contractors the specific procedures for (1) releasing customer records (without prior customer consent), (2) contacting the customer with program information, and (3) ensuring confidentiality of customer-specific information. Utility customer information received through this process may be used only for LIEE purposes. The use of utility customer information for purposes other than LIEE programs and purposes may result in penalties, including, but not limited to revocation of contractor’s or subcontractor’s ability to participate in LIEE programs.<sup>30</sup>

Reciting language from a previous decision (D.93-02-041, the Commission expressed its expectation that PG&E, SDG&E, SCE and SoCal would “negotiate these procedures with winning bidders on a case-by-case basis.”<sup>31</sup> The utilities argument in this proceeding that they should not be held responsible for such negotiations make pursuant to SB 1476 runs counter to precedent.

#### **IV. PRACTICES OF CALIFORNIA UTILITIES.**

Southern California Edison (SCE), Pacific Gas & Electric (PG&E) and San Diego Gas & Electric (SDG&E) each responded to the Assigned Commissioner’s Ruling which asked for information about what usage information is being generated and will be

---

<sup>28</sup> D.09-09-047 at 253-54.

<sup>29</sup> D.09-09-047 at 254

<sup>30</sup> D.00-07-020 at 116-17 (July 12, 2000)

<sup>31</sup> *Id.* at 113, *citing*, D.93-02-041, 48 CPUC2d 199, 209; D.97-12-103, Ordering Paragraph 8.

generated, whether customers can access that data, what privacy protections exist for personal information of customers, who will have access to the data generated by the Smart Meters, and other information, as well. It appears from those responses that utilities are following the practices discussed above, as required by law and Commission decisions.

There are, however, many questions to address with respect to how information is made available to customers and third parties.

A. There Is A Question About Whether The Utility Will Retain The Role Of Caretaker For Customer Usage Data.

All utilities have confirmed that usage data is provided to customers, but not until the day after actual usage. The data provided is cumulative, except where smart meters have been installed.

SCE plans to continue making backhauled information available to customers on a next day basis, displaying that information on the web as a cumulative, bill-to-date amount. At some point in 2012, SCE will begin transmitting near real time usage data to the customers' home area networks (HAN). SCE makes the following statement which needs to be explained: "Note that this information will not be backhauled to the IOU back office systems but will be available from the smart meter, located at the customer's premise, directly to the consumer's registered device."<sup>32</sup>

CFC believes this statement means that SCE will not make usage data available to third parties once its smart meters have been installed and connected to the customer's HAN.<sup>33</sup> SCE says it "is not backhauling the near real-time usage data provided via the HAN; therefore, the customer may elect to share that data with third parties directly."<sup>34</sup> PG&E makes a similar remark: "PG&E's SmartMeter™ enabled Home Area Network ... system, when complete, will provide customers with the ability to access their energy usage data ... using HAN-enabled devices .... The energy

---

<sup>32</sup> See, Attachment to SCE Response Comments at "A-1".

<sup>33</sup> Presumably SCE will continue to need usage information for billing, load management and other purposes after smart meters are installed.

<sup>34</sup> SCE Response Comments at "A-2."

usage data on the HAN system will be provided directly to the customer and in general will not be available on the utility servers.<sup>35</sup>

CFC infers from these statements, and others, in the utilities' Responses and at the workshop, that the utilities intend to refuse requests for customer data once the smart meters start transmitting data to the HAN. This approach has not been justified.

Customers do not have the same bargaining power as a utility, when contracting with an energy management provider, to protect the privacy of customers' personal information, and no amount of certification of third parties will change that. SCE will continue using customer usage data "for billing purposes and to assist customers in selecting rates and programs ... [and] to offer customers energy management tools, such as the web presentment of interval data, bill-to-date, bill forecast, and budget alert tools." And SCE has admitted it has the ability to negotiate with contractors (third parties) to whom data has been given under a promise of confidentiality.<sup>36</sup>

There would appear to be several points at which third parties must interact with the utility. For example, EnerNoc currently obtains "timelier and more granular" usage data through a KYZZ pulse data recorder installed by the utility on the meter. It enters into a contract with the utility establishing terms for installation of the KYZ recorder.<sup>37</sup> On PG&E's system, the third party will have to register its devices with PG&E. (p.2) It would not, therefore, constitute an unreasonable burden to require the utilities to monitor the third parties' use of customer data when it is also going to be monitoring the third party's compliance with the contract signed with the utility.

The Commission should also require that contracts between a utility and a third party be filed with the Commission and approved, before they take effect. The filing should include a copy of any consent document the customer provided and a copy of the notice given the customer which solicited the customer's consent.

#### B. Liability for Information Leaks

SCE appears to be concerned about potential liability if it releases private information to third parties. This, however, is a role that SCE has played for a long time.

---

<sup>35</sup> PG&E Response Comments at

<sup>36</sup> SCE Response Comments at 9.

<sup>37</sup> EnerNoc also enters into a contract with the customer under which it provides real-time usage data to the customer "through a secure, proprietary web portal."

In D.00-07-020, the Commission required the utilities to “negotiate with contractors the specific procedures for (1) releasing customer records (without prior customer consent), (2) contacting the customer with program information, and (3) ensuring confidentiality of customer-specific information.”

The law requires that the utilities monitor third parties’ use of customers private information and imposes liability on them if that duty is not reasonably performed. SCE and other utilities are subject to Civil Code section 1798.81.5(c) which requires that a “business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information . . . .” Section 1798.84(a) states that “[a]ny waiver of a provision of this title is contrary to public policy and is void and unenforceable.” Further subsection (b) states that “[a]ny customer injured by a violation of this title may institute a civil action to recover damages.” Civil penalties are also available in subsection “(c)”.

“SDG&E believes statewide certification of third parties may be prudent to provide minimum protection and oversight of third parties.”<sup>38</sup> The extent of the requirements for obtaining certification is not specified. If certification is required, a careful balance must be struck between making those requirements sufficient to protect customers without excluding all but those with demonstrated experience. Some energy management firms may not have established products, but will be offering innovative technology which would be useful to customers.

Tendril takes umbrage at suggestions that third parties will not adequately protect customers’ personal information. “Several comments (both written and in hearing) allude to the need to protect consumers from the unauthorized disclosure of consumer information. While not always explicitly stated, the implied assumption is that there is a risk of data disclosure that may occur to parties outside of Commission jurisdiction<sup>39</sup> without consumer knowledge or authorization. We fail to find any indication in the record that any party is proposing such disclosure in this proceeding.” That is not the issue. The issue is how to reverse a release, *i.e.* shut the barn door after the horse has

---

<sup>38</sup> SDG&E Response Comments at 9.

<sup>39</sup> CFC has not, in this document, discussed the jurisdictional issue, but will do so in the brief to be filed November 22.

escaped. So long as there is no entity, other than the customer, to monitor third party practices and request an injunction against misuse of customer data, customers have no assurance that personal data will be kept confidential. As stated by TechNet, “the long-term success of smart grid technologies depends upon consumer confidence and respect of their reasonable expectations of privacy and control over who has access to their energy consumption data.”

### C. Protocols and The Cost of Gathering Data?

Another issue to be addressed is the protocol to be used in accessing data from the meter, and the extent to which it will protect customer privacy. The DOE states in “Data Access And Privacy Issues Related To Smart Grid Technologies.” (Oct. 5, 2010) that once protocols are established by NIST, all Smart Grid investments must comply or forfeit federal funds:

DOE understands that NIST has initiated efforts to support standardization of energy usage information with a North American Energy Standards Board (NAESB) standard information model for customer energy usage information and an American Society of Heating, Refrigerating and Air-Conditioning information model for facility energy usage. In addition, other standards supporting implementation of these information models are already under development, including Open ADE (with NAESB) and the Zigbee Smart Energy Profile 2.0. DOE notes that once any protocols or model standards are developed and published by NIST for the interoperability of Smart Grid devices and technologies, an investment that fails to incorporate any of such protocols or model standards is not eligible for reimbursement under the Federal Smart Grid Investment Matching Grant Program. Pub. L. 110-140, Section 1306.

#### 1. *Open ADE or Smart Energy Standards*

SCE states “the IOUs intend to provide customers and authorized third parties with access to backhauled customer usage data through a national standards-based Open ADE process.”<sup>40</sup>

SCE proposes that the Commission authorize the IOUs to offer a data exchange program that adheres to the Open ADE standard under development within the National Institute of Standards and Technology (NIST) and North American Energy Standards Board (NAESB) framework, which includes system and architecture requirements developed to protect the confidentiality, integrity and availability of customer information in

---

<sup>40</sup> SCE Response Comments at 9.

transit and at rest. The Commission should adopt the Open ADE standard, which is expected to be ratified by the NAESB and accepted by NIST by the end of 2010, to ensure that the IOU and third party systems are compatible and interoperable pursuant to national standards. (A-3 to A-4, *emphasis added*)

PGE has not answered that part of Question No. 2, which asked what data exchange rules the utility proposes the Commission adopt. (pp. 3-4) It does make a reference in response to Question No. 1 that it will expect third parties to meet Zigbee Smart Energy 2.0 standards “for access and customer security.” (p.2)

SDG&E offers a somewhat unclear statement about the protocol it intends to use:

A general interface to customer “authorized” third parties cannot be made available by SDG&E until the Open Automated Data Exchange (ADE) standards are established. SEP 2.0 standards are not expected to be finalized until mid-2011. Diverse product availability (e.g., In-home Displays or IHDs) under the SEP 2.0 standards will not be widely available until well into 2012. ... The SDG&E HAN pilots will be utilizing SEP 1.0 protocols. SEP 1.0 devices may not be compatible once the SEP 2.0 standard is implemented.

There are two key interfaces that must be standardized and made “live” as soon as practicable: (1) the online system level interface for sharing data with third parties authorized by the customer and (2) the real-time home area network/ business area network (HAN/BAN) interface to smart meters. (TechNet?) The protocols adopted will affect the ability of third parties to use customers’ energy usage information.

EnerNoc says, “Access to data through the utility server using the OpenADE protocol will not be satisfactory for the types of services EnerNOC provides to its C&I customers,” It needs “raw data collected by the meter; not data that has been verified, edited or enhanced.” . Tendril recommends that the Open ADE protocol be used for the “transfer of historical time-interval data between the utility and the consumer domains” and that the Smart Energy Profile data standard be used for the transfer of real-time information directly from the meter into the consumer domain. TechNet recognizes, however, that “most customers may not require that level of data granularity.” (p.)

The DOE, however, pointed out the tension between third parties' interest in getting as much data as possible *vis à vis* customers' interest in minimizing the amount of data utilities collect, to avoid unnecessary utility expense:

SCE itself does not collect that real-time data: Instead, it backhauls usage data from meters at hourly intervals. This data is then validated and processed to produce the —revenue quality interval usage data□ that SCE uses for billing and providing utility services, and provides to consumers on a next-day basis through SCE's web portal. Therefore, although SCE's smart meters do provide near-real-time data to consumers, SCE warns that it would need to re-engineer its smart-meter system were *SCE itself* required to provide third parties with near-real-time energy-usage data, or —revenue-quality□ interval-usage data on other than a next-day basis.

This example illustrates a potentially critical point. Utilities can promote the innovation that Smart Grid technologies enable by serving as least-cost providers of a potentially vast array of data including current and historic CEUD that they actually collect and maintain. But to the extent that utilities are required to collect or retain data exceeding that required to provide efficient electric power generation, transmission and delivery services to their particular customers without charging for such access, this requirement threatens to distort the cost of electric power *vis a vis* that of third-party services.<sup>41</sup>

Utilities should not be used to subsidize the energy management industry. The cost of electricity is high enough in California without requiring utilities to collect data they do not need, at customers' expense. This is particularly true now, when customers are still recovering from a seriously recessionary economy. So long as the utility provides sufficient data to enable the customer to manage his or her energy use, the cost of collecting any additional data for third parties should be assessed to the third party.

## 2. *Security Measures, Now and in the Future*

No one disputes the Commission's authority to require utilities to adopt appropriate security protocols which will insure that usage data can be accessed only by authorized persons and for authorized purposes at all stages of capture, transport, storage, and use. There are protections already in place.

Many noted that current utility cyber controls already help prevent such unauthorized access. Such controls could include data encryption and secure maintenance of encryption keys, network segmentation, the

---

<sup>41</sup> DOE, "Data Access And Privacy Issues Related To Smart Grid Technologies." (Oct. 5, 2010) at 20). [http://www.gc.energy.gov/documents/Broadband\\_Report\\_Data\\_Privacy\\_10\\_5.pdf](http://www.gc.energy.gov/documents/Broadband_Report_Data_Privacy_10_5.pdf)

separation of operational and other data from customer data, appropriate controls on employee access to data and employee training on proper data handling, clear authorization procedures for third party access to customer data, authentication of Smart Grid devices and users, intrusion detection and prevention, physical security controls, and auditing procedures, among others.<sup>42</sup>

SDGE discussed in its comments and at the workshops the unique customer identifier it uses when providing customer energy usage data to Google.

Whatever can be done to protect personal information should be done.<sup>43</sup> Authors of an article "*Legal Aspects of Data Security*"<sup>44</sup> recommend several steps that can be taken by business to secure customer information:

- Limit the information collected and stored.
- Limit access to data.
- Encrypt data
- Audit personal information for accuracy and protection.
- Centralize data for better control and make subject to uniform security mechanisms
- Develop notification procedures.
- Respond to breaches
- Review third party agreements.

The price of not securing consumer information is steep.<sup>45</sup> Further discussion is needed on the subject of the security procedures now in place at each of the utilities and of the security.

Further, some investigation should be undertaken about the security protections included in the two protocols which have been proposed for transferring data. SCE describes a "data exchange program that adheres to the Open ADE standard under development within the National Institute of Standards and Technology (NIST) and North American Energy Standards Board (NAESB) framework," which, it says, "includes system and architecture requirements developed to protect the confidentiality, integrity

---

<sup>42</sup> *Id.* at 46.

<sup>43</sup> See generally, Cal. Civ. Code § 1798.81.5, 1798.82.

<sup>44</sup> Daily Journal: M. Lindsey and J. Sabatini, *Legal Aspects of Data Security*.

<http://www.dailyjournal.com/cle.cfm?show=CLEDisplayArticle&qVersionID=81&eid=860757&eid=1>

<sup>45</sup> R. Gellman, *How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete* (March 2002)

and availability of customer information in transit and at rest.”<sup>46</sup> These protections should be more fully discussed. Proponents of Smart Energy protocols have not explained what security provisions are built into the protocols. CFC is not aware of any information in the record on which the Commission could base a finding that adoption of one or more of these protocols would adequately safeguard customer information. More information is needed.

D. The Potential for Anti-Competitive Behavior.

There would appear to be several points at which third parties must interact with the utility. The Commission must be careful, to prevent utilities from using the power to determine access, e.g., eligibility and set up, as a means to limit the amount of competition by third parties for the customer’s business.

For example, in addition to registration and installation of devices on the meter, SCE suggests the Commission might want a tariff developed to set the contours of the Open ADE program. The tariff proposed by SCE “would set forth the rights and obligations of the data exchange parties including:

- Eligibility and set-up – including necessary technical functionalities
- Customer authorization for third party access
- Third party registration
- Data transmittal
- Customer and third party indemnifications.”

Another barrier to entry may be the utility’s limitation of access to itself or a single energy management provider, as appears to be the case currently, with SDG&E: “SDG&E currently provides customer access to their Smart Meter interval usage data via the Google PowerMeter. SDG&E is expected to provide residential customers with access via SDG&E’s MyAccount by early 2011.”

---

<sup>46</sup> SCE Comments at A-3 & A-4.

## ATTACHMENT I

### **Privacy Practices Recommendations:**

**Assign privacy responsibility.** Each organization collecting or using Smart Grid data from or about consumer locations should create (or augment) a position or person with responsibility to ensure that privacy policies and practices exist and are followed. Responsibilities should include documenting, ensuring the implementation of, and managing requirements for regular training and ongoing awareness activities.

**Establish privacy audits.** Audit functions should be modified to monitor all energy data access.

**Establish law enforcement request policies and procedures.** Organizations accessing, storing, or processing energy data should include specific documented incident response procedures for incidents involving energy data.

**2. Notice and Purpose:** A clearly specified notice should exist and be shared in advance of the collection, use, retention, and sharing of energy data and personal information.

### **Findings:**

The data obtained from systems and devices that are part of the Smart Grid and accompanying potential and actual uses for that data create the need for organizations to be more transparent and clearly provide notice documenting the types of information items collected and the purposes for collecting the data.

### **Privacy Practices Recommendations:**

**Provide notification for the personal information collected.** Any organization collecting energy data from or about consumers should establish a process to notify consumer account inhabitants and person(s) paying the bills (which may be different entities), when appropriate, of the data being collected, why it is necessary to collect the data, and the intended use, retention, and sharing of the data. This notification should include information about when and how information may or may not be shared with law enforcement officials. Individuals should be notified before the time of collection.

**Provide notification for new information use purposes and collection.** Organizations should update consumer notifications whenever they want to start using

existing collected data for materially different purposes other than those the consumer has previously authorized. Also, organizations should notify the recipients of services whenever they want to start collecting additional data beyond that already being collected, along with providing a clear explanation for why the additional data is necessary.

**3. Choice and Consent:** The organization should describe the choices available to consumers with regard to the use of their associated energy data that could be used to reveal personal information and obtain explicit consent, if possible, or implied consent when this is not feasible, with respect to the collection, use, and disclosure of this information.

**Findings:**

Currently it is not apparent that utilities or other entities within the Smart Grid obtain consent to use the personal information generated and collected for purposes other than billing. As smart meters and other smart devices increase capabilities and expand sharing of the data throughout the Smart Grid, organizations should establish processes to give consumers a choice, where possible and feasible, about the types of data collected and how it is used.

**Privacy Practices Recommendation:**

**Provide notification about choices.** The consumer notification should include a clearly worded description to the recipients of services notifying them of (1) any choices available to them about information being collected and obtaining explicit consent when possible; and (2) explaining when and why data items are or may be collected and used without obtaining consent, such as when certain pieces of information are needed to restore service in a timely fashion.

**4. Collection and Scope:** Only personal information that is required to fulfill the stated purpose should be collected from consumers. This information should be obtained by lawful and fair means and, where appropriate and possible, with the knowledge or consent of the data subject.

**Findings:**

In the current operation of the electric utilities, data taken from traditional meters consists of basic data usage readings required to create bills. Under the Smart Grid

implementation, smart meters will be able to collect other types of data. Home power generation services will also likely increase the amount of information created and shared. Some of this additional data may constitute personal information or may be used to determine personal activities. Because of the associated privacy risks, only the minimum amount of data necessary for services, provisioning, and billing should be collected.

**Privacy Practices Recommendations:**

**Limit the collection** of data to only that necessary for Smart Grid operations, including planning and management, improving energy use and efficiency, account management, and billing.

**Obtain the data** by lawful and fair means and, where appropriate and possible, with the knowledge or consent of the data subject.

**5. Use and Retention:** Information within the Smart Grid should be used or disclosed only for the purposes for which it was collected. Smart Grid data should be aggregated in such a way that personal information or activities cannot be determined, or anonymized wherever possible to limit the potential for computer matching of records. Personal information should be kept only as long as is necessary to fulfill the purposes for which it was collected.

20 NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0 – Aug 2010

**Findings:**

In the current operation of the electric utilities, data taken from traditional meters is used to create consumer bills, determine energy use trends, and allow consumers to control their energy usage both on-site and remotely. The Smart Grid will provide data that can be used in additional ways not currently possible.

**Privacy Practices Recommendations:**

**Review privacy policies and procedures.** Every organization with access to Smart Grid data should review existing information security and privacy policies to determine how they may need to be modified. This review should include privacy

policies already in place in other industries, such as financial and healthcare, which could provide a model for the Smart Grid.

**Limit information retention.** Data, and subsequently created information that reveals personal information or activities from and about a specific consumer location, should be retained only for as long as necessary to fulfill the purposes that have been communicated to the energy consumers. When no longer necessary, consistent with data retention and destruction requirements, the data and information, in all forms, should be irreversibly destroyed. This becomes more important as energy data becomes more granular, more refined, and has more potential for commercial uses.

**6. Individual Access:** Organizations should provide a process to allow for individuals to request access to see their corresponding personal information and energy data, and to request the correction of real or perceived inaccuracies. Personal information individuals should also be informed about parties with whom their associated personal information and energy data has been shared.

**Findings:**

In the current operation of the electric utilities, data may be manually read from the meters. Consumers also have the capability to read the meters through physical access to the meters. Under a Smart Grid implementation, smart meter data may be stored in multiple locations to which the consumer may not have ready access.

**Privacy Practices Recommendations:**

**Consumer access.** Any organization possessing energy data about consumers should provide a process to allow consumers access to the corresponding energy data for their utilities account.

**Dispute resolution.** Smart Grid entities should establish documented dispute resolution procedures for energy consumers to follow.

**7. Disclosure and Limiting Use:** Personal information should not be disclosed to any other parties except those identified in the notice and only for the purposes originally specified or with the explicit informed consent of the service recipient.

**Findings:**

As Smart Grid implementations collect more granular and detailed information, this information is capable of revealing activities and equipment usage in a given location.

As

21 NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0 – Aug 2010

this information may reveal business activities, manufacturing procedures, and personal activities, significant privacy concerns and risks arise when the information is disclosed without the knowledge, consent, and authority of the individuals or organizations to which the information applies.

**Privacy Practices Recommendation:**

**Limit information use.** Data on energy or other Smart Grid service activities should be used or disclosed only for the authorized purposes for which it was collected.

**Disclosure.** Data should be divulged to or shared only with those parties authorized to receive it and with whom the organizations have told the recipients of services it would be shared.

8. **Security and Safeguards:** Smart Grid energy data and personal information, in all forms, should be protected from loss, theft, unauthorized access, disclosure, copying, use, or modification.

**Findings:**

Smart Grid data may be transmitted to and stored in multiple locations throughout the Smart Grid. Establishing strong security safeguards is necessary to protect energy data from loss, theft, unauthorized access, disclosure, copying, use, or modification.

**Privacy Practices Recommendations:**

**Associate energy data with individuals only when and where required.** For example only link equipment data with a location or consumer account when needed for billing, service restoration, or other operational needs. This practice is already common in the utility industry and should be maintained and applied to all entities obtaining or using this data as the Smart Grid is further deployed.

**De-identify information.** Energy data and any resulting information, such as monthly charges for service, collected as a result of Smart Grid operations should be aggregated and anonymized by removing personal information elements wherever possible to ensure that energy data from specific consumer locations is limited appropriately. This may not be possible for some business activities, such as for billing.

**Safeguard personal information.** All organizations collecting, processing, or handling energy data and other personal information from or about consumer locations should ensure that all information collected and subsequently created about the recipients of Smart Grid services is appropriately protected in all forms from loss, theft, unauthorized access, disclosure, copying, use, or modification. While this practice is commonly in effect in the utility industry, as other entities recognize commercial uses for this information, they too should adopt appropriate requirements and controls. In addition, given the growing granularity of information from Smart Grid operations, the responsibility for these existing policies should be reviewed and updated as necessary.

**Do not use personal information for research purposes.** Any organization collecting energy data and other personal information from or about consumer

22 NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0 – Aug 2010

48 Using its authority under Section 5 of the FTC Act, which prohibits unfair or deceptive practices, the Federal Trade Commission has brought a number of cases to enforce the promises in privacy statements, including promises about the security of consumers' personal information.

locations should refrain from using actual consumer data for research until it has been anonymized and/or sufficiently aggregated to assure to a reasonable degree the inability to link detailed data to individuals. Current and planned research is being conducted both inside and outside the utility industry on the Smart Grid, its effects upon demand response, and other topics. The use of actual information that can be linked to a consumer in this research increases the risk of inadvertent exposure via traditional information sharing that occurs within the research community.

**9. Accuracy and Quality:** Processes should be implemented by all businesses participating within the Smart Grid to ensure as much as possible that energy data and

personal information are accurate, complete, and relevant for the purposes identified in the notice [see §5.4.2-2], and that it remains accurate throughout the life of the energy data and personal information while within the control of the organization.

**Findings:**

The data collected from smart meters and related equipment will potentially be stored in multiple locations throughout the Smart Grid. Smart Grid data may be automatically collected in a variety of ways. Establishing strong security safeguards will be necessary to protect the information and the information's accuracy. Since Smart Grid data may be stored in many locations, and therefore be accessed by many different individuals/entities and used for a wide variety of purposes, personal information may be inappropriately modified. Automated decisions about energy use could be detrimental for consumers (e.g., restricted power, thermostats turned to dangerous levels, and so on) if it happens that decisions about energy usage are based upon inaccurate information.

**Privacy Practices Recommendation:**

**Keep information accurate and complete.** Any organization collecting energy data from or about consumer locations should establish policies and procedures to ensure that the Smart Grid data collected from and subsequently created about recipients of services is accurate, complete, and relevant for the identified purposes for which they were obtained, and that it remains accurate throughout the life of the Smart Grid data within the control of the organization.

**10. Openness, Monitoring, and Challenging Compliance:** Privacy policies should be made available to service recipients. These service recipients should be given the ability to review and a process by which to challenge an organization's compliance with the applicable privacy protection legal requirements, along with the associated organizational privacy policies and the organizations' actual privacy practices.<sup>48</sup>

**Findings:**

Currently electric utilities follow a wide variety of methods and policies for communicating to energy consumers how energy data and personal information is used. The data collected from smart meters and related Smart Grid equipment will

potentially be stored in multiple locations throughout the Smart Grid, possibly within multiple states

23 NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0 – Aug 2010

and outside the United States. This complicates the openness of organizational privacy compliance and of a consumer being able to challenge the organization's compliance with privacy policies, practices, and applicable legal requirements.

**Privacy Practices Recommendations:**

**Policy challenge procedures.** Organizations collecting energy data, and all other entities throughout the Smart Grid, should establish procedures that allow Smart Grid consumers to have the opportunity and process to challenge the organization's compliance with their published privacy policies as well as their actual privacy practices.

**Perform regular privacy impact assessments.** Any organization collecting energy data from or about consumer locations should perform periodic PIAs with the proper time frames, to be determined by the utility and the appropriate regulator, based upon the associated risks and any recent process changes and/or security incidents. The organizations should consider sending a copy of the PIA results for review by an impartial third party and making the results of the review public. This will help to promote compliance with the organization's privacy obligations and provide an accessible public record to demonstrate the organization's privacy compliance activities. Organizations should also perform a PIA on each new system, network, or Smart Grid application and consider providing a copy of the results in similar fashion to that mentioned above.

**Establish breach notice practices.** Any organization with Smart Grid data should establish policies and procedures to identify breaches and misuse of Smart Grid data, along with expanding or establishing procedures and plans for notifying the affected individuals in a timely manner with appropriate details about the breach. This becomes particularly important with new possible transmissions of billing information

between utilities and other information between utilities and other entities providing services in a Smart Grid environment (e.g., third-party service providers).

NISTIR 7628 Guidelines for Smart Grid Cyber Security vol. 2, p. 19 (Aug 2010)

## **V. Reply Comments for Providing Pricing Information**

### **A. Background**

The Ruling of September 27, 2010 discussed providing electricity price information to customers. Section 3.5 of the Ruling stated the following:

“Decision (D.) 09-12-046 set as a policy goal providing consumers with access to electricity price information by the end of 2010. At the PHC, several parties noted that since residential prices vary with consumption, it is unclear what price to communicate with customers. For example, should the utility communicate a price to a customer which forecasts his monthly level of consumption, or should the price communicated simply vary depending on the aggregate consumption to date?”

The Assigned Commissioner invited proposals from parties due at the time of opening responses. These proposals were followed by workshops on October 25 and 26, where parties had a chance to discuss their proposals.

### **B. Summary of Viewpoints regarding pricing information**

There was a general consensus among the parties that pricing information provided to customers should be relevant and actionable.<sup>47</sup> There was also some concern that providing real time prices to customers may be unproductive at the moment given the tiered rate structure.<sup>48</sup>

---

<sup>47</sup> Turn Opening Response, October 15, 2010 at 13; SCE Opening Response, October 15, 2010, at 14; DRA Opening Response, October 15, 2010 at 3; CFC Opening Response, October 15, 2010 at page 4.

<sup>48</sup> SCE Opening Response at 13.

TURN stated in its opening response comments that its “primary recommendation has been that the utilities provide residential customers tier alert notifications through email, text or robocall when the customer’s usage crosses into a higher tier, together with a simple statement identifying the price in the next tier.”<sup>49</sup> CFC agrees with TURN that residential customers should receive automated alerts delivered via email, phone, or text messaging. CFC believes, however, that tier alert notification will not be as useful as a message communicating the amount customers will be billed (price times usage). In the former scenario, a customer still has to calculate how many kilowatts he or she has used for a particular tier and multiply it by the price associated with that tier. This will prove to be confusing for the average customer.

### **C. Utilities’ Pricing Proposals**

CFC overall agreed with SCE’s pricing proposals. CFC particularly liked SCE’s proposal to provide bill-to-date and bill forecast information to its SmartConnect customers on SCE.com. CFC also supports SCE providing alerts which will notify the customer by voice, text, or email when a customer will exceed their preset budget amount.<sup>50</sup> CFC believes that providing the customer with an already calculated result of both cumulative energy usage and applicable rate, as opposed to directing the customer to decipher complicated raw data will be the relevant, actionable information necessary for the customer to make smart decisions concerning their energy usage and bill.

It is unclear in SCE’s proposal how many times per billing cycle a customer will be able to receive these calculated amounts. CFC understands that these details will most likely be fleshed out in the implementation phase, however, CFC respectfully requests that a customer be able to get updated calculations multiple times per day.

Among the utility proposals, CFC was least impressed with PG & E’s proposal. When asked to provide a proposal, PG & E responded that it is *already* providing

---

<sup>49</sup> Turn Opening Response at 13.

<sup>50</sup> SCE Opening Response at 14.

electricity pricing information to individual customers in conjunction with their SmartMeter energy usage data.<sup>51</sup> This answer suggests that PG & E is resistant to change its current method of providing information to customers which is confusing and of little value to the customer.

Currently, PG & E provides general information on a public website. This information is not customized or tailored specifically to a particular customer.<sup>52</sup> Customers who wish more specific rate information have to assume the burdensome task of calling a PG & E customer service representative to get information regarding their specific rate.<sup>53</sup> Anyone who has dealt with telephone customer service knows that this can be timely, labor intensive, confusing, and sometimes of little result to the customer. As such, this method strains customer access to their specific pricing information rather than encouraging it. CFC believes that PG & E can institute measures that facilitate access to pricing information as it relates to a particular customer's energy usage cost effectively.

---

<sup>51</sup> PG & E Opening Response, October 15, 2010 at 5.

<sup>52</sup> PG & E Opening Response at 5.

<sup>53</sup> Id.

In short, CFC does not understand why PG&E is hesitant to update their antiquated method of providing pricing information which does nothing more than perpetuate consumer barriers rather than remove them. CFC respectfully requests that PG&E take an active step in changing its approach to providing pricing information to customers.

Dated November 8, 2010

Respectfully submitted,

By: \_\_\_\_\_ //s//

and

By: \_\_\_\_\_ //s//

Alexis K. Wodtke  
520 S. El Camino Real, Suite 340  
San Mateo, CA 94402  
Phone: (650) 375-7840  
Fax: (650) 343-1238  
Email: lex@consumercal.org

Nicole A. Blake  
520 S. El Camino Real, Suite 340  
San Mateo, CA 94402  
Phone: (650) 375-7845  
Fax: (650) 343-1238  
Email: blake@consumercal.org



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  
bobsmithtl@gmail.com  
mtierney-lloyd@enernoc.com  
ed@megawattsf.com  
mterrell@google.com  
mdjoseph@adamsbroadwell.com  
cbreakstone@control4.com  
elaine.duncan@verizon.com  
pickering@energyhub.net  
margarita.gutierrez@sfgov.org  
lms@cpuc.ca.gov  
fsmith@sflower.org  
srovetti@sflower.org  
tburke@sflower.org  
marcel@turn.org  
mkurtovich@chevron.com  
cjh5@pge.com  
david.discher@att.com  
nes@a-klaw.com  
harold@seakayinc.org  
pcasciato@sbcglobal.net  
steven@sflower.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  
jody\_london\_consulting@earthlink.net  
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  
jurban@law.berkeley.edu  
kerry.hattevik@nrgenergy.com  
rquattrini@energyconnectinc.com  
michael\_w@copper-gate.com  
diana@aspectlabs.com  
TGlasse@Certichron.com  
seboyd@tid.org  
dzlotlow@caiso.com  
dennis@ddecuir.com  
scott.tomashefsky@ncpa.com  
jhawley@technet.org  
Inavarro@edf.org  
Lesla@calcable.org  
cbk@eslawfirm.com  
mcoop@homegridforum.org  
cassandra.sweet@dowjones.com  
dblackburn@caiso.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  
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  
jorgecorralej@sbcbglobal.net  
dschneider@lumesource.com  
lmitchell@hanmor.com  
david@nemtzw.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  
kмкиener@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  
faramarz@ieee.org  
rudy.reyes@verizon.com  
mandywallace@gmail.com

norman.furuta@navy.mil  
kgrenfell@nrdc.org  
nsuetake@turn.org  
bfinkelstein@turn.org  
mcarboy@signalhill.com  
andrew\_meiman@newcomb.cc  
regrelcpuccases@pge.com  
dpb5@pge.com  
DNG6@pge.com  
filings@a-klaw.com  
Kcj5@pge.com  
mpa@a-klaw.com  
michelle.choo@att.com  
rcounihan@enernoc.com  
sls@a-klaw.com  
stephanie.holland@att.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  
mariacarbhone@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  
uzma@crve.org  
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@gmail.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  
cmkehrrein@ems-ca.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  
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  
roger147@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  
lft@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