



FILED

12/06/10  
04:59 PM

BEFORE THE PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIFORNIA

Order Instituting Rulemaking to Consider  
Smart Grid Technologies Pursuant to  
Federal Legislation and on the  
Commission's own Motion to Actively  
Guide Policy in California's Development  
of a Smart Grid System.

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

**REPLY BRIEF OF THE CONSUMER FEDERATION OF CALIFORNIA  
CONCERNING THE COMMISSION'S AUTHORITY  
OVER RECIPIENTS OF CONSUMER USAGE DATA.**

**I. INTRODUCTION**

Californians have a Constitutional right to privacy.<sup>1</sup> That right has been repeatedly construed to provide California citizens with privacy protections broader than those recognized by the federal Constitution.<sup>2</sup> The investor-owned utilities have been directed by the legislature to prevent the disclosure of utility customers' "electrical or gas consumption data." They are prohibited from disclosing the information to third parties unless the third party signs a contract promising to protect utility customers' privacy.

Nothing in this section shall preclude an electrical corporation or gas corporation from disclosing a customer's electrical or gas consumption data to a third party for system, grid, or operational needs, or the implementation of demand response, energy management, or energy efficiency programs, provided that, for contracts entered into after January 1, 2011, the utility has required 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, and prohibits the use of the data for a secondary commercial purpose not related to the primary purpose of the contract without the customer's consent.<sup>3</sup>

The issue of the Commission's jurisdiction over third parties would not arise if the utilities would perform the duties required by Public Utilities Code section 8380.

<sup>1</sup> California Constitution, art. I, § 1, See e.g., Sheehan v. San Francisco 49ers, Ltd., 45 Cal. 4th 992

<sup>2</sup> Jeffrey H. v. Imai, Tadlock & Keeney, 85 Cal. App. 4th 345, 353 (Cal. App. 1st Dist. 2000)

<sup>3</sup> Pub. Util. Code § 8380(a) & (b)

However, since it has, this Reply Brief demonstrates that the utilities' arguments limiting the Commission's jurisdiction are without substance.

CFC also examines the statutes cited by San Diego Gas & Electric and SoCal Gas and has identified important elements common to other privacy statutes, which it proposes by incorporated in rules adopted by the Commission.

#### A. PACIFIC GAS & ELECTRIC

PG&E argues that agents of the utility are the only third parties over whom the Commission may exercise jurisdiction, as exemplified by an examination of penal statutes.<sup>4</sup> The statutes it cites do not support its argument. Although Sections 2009 and 2110 apply only to "an officer, agent, or employee of any public utility" (§ 2009) or "[e]very public utility and every officer, agent, or employee of a public utility" (Pub. Util. Code § 2110), the sections which follow identify other miscreants which are not officers agents or employees of a public utility.

2111. Every corporation or person, other than a public utility and its officers, agents, or employees, which or who knowingly violates or fails to comply with, or procures, aids or abets any violation of any provision of the Constitution of this state relating to public utilities or of this part ... is subject to a penalty of not less than five hundred dollars (\$500), nor more than twenty thousand dollars (\$20,000) for each offense.

2112. Every person who, either individually, or acting as an officer, agent, or employee of a corporation other than a public utility, violates any provision of this part, ... is guilty of a misdemeanor, and is punishable by a fine not exceeding one thousand dollars (\$1,000), or by imprisonment in a county jail not exceeding one year, or by both such fine and imprisonment.."<sup>5</sup>

The inclusion of the phrase "other than a public utility" indicates the legislature intended that non-utilities be sanctioned for violations of utility laws and regulations.

PG&E also argues that because Pub. Util. Code "section 8380 confers authority on the Commission to directly regulate utilities but not their non-utility agents and contractors," "the Legislature intends the Commission to only regulate utilities on

---

<sup>4</sup> PG&E Brief on Jurisdiction at 3.

<sup>5</sup> See, SDG&E/SoCal Jurisdiction Brief at 5.

these matters.”<sup>6</sup> The premise of its argument is wrong, since the legislature clearly intended that others be subject to the Commission’s jurisdiction (see, above).

Second, PG&E uses “the canon of statutory construction *expressio unius est exclusio alterius*,” to show that “the Legislature intends the Commission to only regulate utilities on these matters. “[T]he application of this statutory construction tool to an entire code is questionable.”<sup>7</sup> PG&E’s attempt to relate section 8380 to Pub. Util Code section 2112 must be deemed of similar questionable value. The maxim *expressio unius est exclusio alterius* is generally applied to a specific statute, which contains a listing of items to which the statute applies.”<sup>8</sup>

Third, courts have indicated they will ignore the maxim *expressio unius est exclusio alterius* where, for example “its operation would contradict a discernible and contrary legislative intent.”<sup>9</sup>

It is clear from the review of the Public Utility Code and privacy statutes, discussed below and in the Appendix, that the legislature intended any entity in possession of personal information be held to the same standards as the utilities. The Legislature was aware of the practice of third parties purchasing personal information of a customer from the entity which gathered it. Many of the statutes summarized in the Appendix to this brief regulate the conduct of third parties indirectly through the entity in possession of personal information, by requiring that entity to enter into a contract, before releasing the data, which requires the third party to keep the information secure

---

<sup>6</sup> PG&E Jurisdiction Brief at 4.

<sup>7</sup> *In re Sabrina H.* (2007) 149 Cal. App. 4th 1403, 1411.

<sup>8</sup> *In re Sabrina H.* (2007) 149 Cal. App. 4th 1403, 1411

<sup>9</sup> 149 Cal. App. 4th at 1412 . The court identified other circumstances in which the rule would not be applied: “[E]xpressio unius est exclusio alterius is no magical incantation, nor does it refer to an immutable rule. Like all such guidelines, it has many exceptions . . . .” The high court listed some of the exceptions as follows: “The rule is inapplicable: where no manifest reason exists why other persons or things than those enumerated should not be included and thus exclusion would result in injustice [citation]; to a statute the language of which may fairly comprehend many different objects, some of which are mentioned merely by way of example, without excluding others of similar nature [citation]; to a matter which is only incidentally dealt with in a statute [citation]; where its application would run counter to a well established principle of law.” 149 Cal. App. 4<sup>th</sup> at 1412, *citing*, *People v. Reed* (1996) 13 Cal.4th 217, 227 ; *Estate of Banerjee* (1978) 21 Cal.3d 527, 539.

and private. There is no indication in SB 1476 that the legislature intended to specially repeal the Information Practices Act of 1977<sup>10</sup> for utilities.

PG&E argues that an analysis of the Commission's jurisdiction over third parties should not be ended if regulation of third parties is found to be cognate and germane to utility regulation because there are "other laws and statutes, both state and federal, that "may conflict with direct Commission regulation of non-utilities in this area," leaving a court no choice but to strip the Commission of jurisdiction altogether.<sup>11</sup> PG&E ignores the rule of statutory construction that "it is fundamental that legislation should be construed so as to harmonize its various elements without doing violence to its language or spirit."<sup>12</sup>

Further, there is no conflict between Pub. Util. Code section 8380 and other privacy statutes. Other statutes do not identify customer consumption data as non-public personal information to be protected. Section 8380, on the other hand, is entitled "Privacy Protections for Energy Consumption Data" and prohibits disclosure of a customer's electrical or gas consumption data. Section 8380 does not serve the same interest in protecting information that could be used to identify an individual and thereby violate a person's right to privacy.

Even if there were a conflict among privacy statutes, conflict is apparently tolerated by the legislature (and the courts). For example, Civil Code section 1785.11.2 puts the burden on customers to request confidentiality by allowing disclosure of a credit report unless a customer asks for a freeze on disclosure. Civil Code section 1798.24(b), on the other hand, puts the burden on a business in possession of personal information to obtain customer consent. The business may not release personal information without "prior written voluntary consent" of the consumer.

PG&E attempts to distinguish the Commission's jurisdiction over non-utility *agents* of the utility from its jurisdiction over non-utility *companies*.<sup>13</sup> It argues the Commission's does not have jurisdiction over third parties "where the non-utility access to the information is not contractual." The point missed in its argument is that in order to

---

<sup>10</sup> Pub. Util. Code section 1798 *et. seq*

<sup>11</sup> PG&E Jurisdiction Br. at 4-5.

<sup>12</sup> People v. Garcia, 21 Cal. 4th 1, 6 (Cal. 1999)

<sup>13</sup> PG&E Jurisdiction Br. at 5.

obtain information from the utility, the third party must by contract agree that the information will be kept confidential.<sup>14</sup> Thus, the non-utility company's access to personal information held by the utility is contractual.

When addressing the situation where a third party obtains consumption data from the customer (not the utility), PG&E recognizes that the Commission could attempt to indirectly regulate the handling of information obtained from the customer.<sup>15</sup> Southern California Edison (SCE) also recognizes "the Commission has full authority to approve the terms and conditions under which the IOUs are permitted to release customer data to such third parties."<sup>16</sup> SDG&E and SoCal recognize the Commission could direct the utility "to interrupt or cutoff the flow of utility information regarding a consumer's energy usage" where the third party is not adequately protecting the data.<sup>17</sup>

The Commission could also indirectly regulate the release of consumption data by prohibiting access to metered data pursuant to the authority granted by Pub. Util. Code section 761.

Whenever the commission, after a hearing, finds that the rules, practices, equipment, appliances, facilities, or service of any public utility, or the methods of manufacture, distribution, transmission, storage, or supply employed by it, are unjust, unreasonable, unsafe, improper, inadequate, or insufficient, the commission shall determine and, by order or rule, fix the rules, practices, equipment, appliances, facilities, service, or methods to be observed, furnished, constructed, enforced, or employed.

The Commission may find that a public utility's practice of releasing information to third parties is unjust, unreasonable and improper, and order utilities to institute a procedure which makes any third party obtaining consumption data from the utility abide by the Commission's privacy rules.

The Commission also has authority to "prescribe reasonable regulations for the examination and testing of the product, ..., or service and for the measurement thereof."<sup>18</sup> In most instances, the customer obtains usage data from the smart meter. Access to the meter is necessary to obtain information the customer will pass on to third

<sup>14</sup> Pub. Util. Code § 8380(e)(2)

<sup>15</sup> PG&E Jurisdiction Br. at 8.

<sup>16</sup> SCE Jurisdiction Br. at 9.

<sup>17</sup> SDG&E/SoCal Jurisdiction Br at 7-8.

<sup>18</sup> Pub. Util Code § 770(c)

parties. The Commission could find that it would be unjust, unreasonable and improper for data to be taken from public utility meters if customers and through them, third parties were allowed access to consumption data without first agreeing to abide by privacy rules of the Commission.<sup>19</sup> The customer's access to usage data in the detail desired by third parties could be used as a bargaining chip to achieve the same degree of protection for customers whether their consumption data is passed on by the utility or by the customer.

## **B. SOUTHERN CALIFORNIA EDISON**

Southern California Edison (SCE) claims "the IOUs have no reasonable means of investigating or verifying suspected misuse of customer energy usage data by customer-authorized third parties, or adjudicating or enforcing such matters."<sup>20</sup> The statement is somewhat ambiguous. SCE should provide further explanation because there appear to be a number of means by which SCE could investigate misuse of customer data. If SCE means it doesn't have the money it needs to investigate, that can be rectified in its current rate filing. SCE could create a procedure for customers to complain about mishandling of the data (e.g., using the data to market a product), and investigate those claims. In the absence of proof to the contrary, it appears that if SCE wanted to investigate data misuse, it could find ways to do so.

SCE says it "prefers to allow its customers to continue to have the responsibility for monitoring and managing the use of data by their authorized third parties, as is the case today for customer authorized releases of data from the IOUs."<sup>21</sup> In order to monitor and manage the consumption data, however, the customer would have to be given the right to make sure the meter is providing accurate information, to test the meter and have it fixed, if necessary.<sup>22</sup> The accuracy of data registered by the meter is critical in the energy management process. The utilities have not offered to give up control of their meters.

---

<sup>19</sup> Pub. Util. Code § 761

<sup>20</sup> SCE Jurisdiction Br. at 9.

<sup>21</sup> SCE Jurisdiction Br. at 10.

<sup>22</sup> In R.06-03-004, the utilities argued they should be the provider of meters and be responsible for making sure that the meter meets the Commission's standards. See e.g., May 26, 2006, Comments of San Diego Gas & Electric at 21.

“SCE recommends that the Commission direct the IOUs to work collaboratively to prepare draft Open Automated Data Exchange (ADE) tariffs that include terms for customer consent, termination of consent, indemnification, etc., along with the operational and technical requirements for parties accessing data through Open ADE, and then hold a workshop to discuss the drafts.”<sup>23</sup> SCE’s assumption of responsibility for deciding how data will be exchanged, on behalf of utilities, is incongruent with the policy of the smart grid, *i.e.*, making access open and available to all.

ADE (aka Electric Data Interchange) “can be formally defined as ‘The transfer of structured data, by agreed message standards, from one computer system to another without human intervention’.”<sup>24</sup> The National Institute of Standards and Technology “defines electronic data interchange as ‘the computer-to-computer interchange of strictly formatted messages that represent documents other than monetary instruments.’ EDI implies a sequence of messages between two parties, either of whom may serve as originator or recipient.”<sup>25</sup> If the utility is exchanging data with a customer or a third party, all parties should be engaged in discussions of the ‘operational and technical requirements for parties accessing data through Open ADE.’ Customers and privately funded businesses may not have the wherewithal to support the purchase of all the bells and whistles associated with a utility-preferred system.

SCE argues that rather than enforcing state laws protecting customers’ privacy, the Commission should “direct the IOUs to engage in appropriate education and outreach efforts to help empower customers to protect themselves from misuse of energy usage and other data gathered through customer HANs.”<sup>26</sup> Education provided by a utility may be biased.

The likelihood that a utility can impartially “inform customers that they are not obligated to authorize third party data access because they can access energy usage data and other energy management tools from their IOUs”<sup>27</sup> is slim. Look at PG&E’s efforts to ‘educate’ consumers in Marin County, San Francisco and the San Joaquin Valley about community choice aggregation. According to a Marin County Supervisor,

---

<sup>23</sup> SCE Jurisdiction Br. at 10.

<sup>24</sup> WIKIPEDIA: Electronic Data Interchange

<sup>25</sup> *Id.*

<sup>26</sup> SCE Jurisdiction Br. at 11.

<sup>27</sup> *Id.*

“PG&E met Marin’s efforts [to establish community choice] with a skillfully executed misinformation campaign.”<sup>28</sup> The general manager of the San Joaquin Valley Power Authority described PG&E’s response to formation of the Authority as “a continuum of opposition and non-cooperation.”<sup>29</sup> Utilities have their own interests to protect. Any educational outreach should be performed by the Commission or a neutral and qualified agency.

### **C. SAN DIEGO GAS & ELECTRIC and SOCAL GAS.**

San Diego Gas & Electric and SoCal Gas argue there is sufficient regulation of customers’ privacy because there are “extensive state and federal regulations and statutes that already address the misuse of customer data,” consumer protections are “already appropriately addressed” and therefore, should not be duplicated by the Commission. An attachment to SDG&E’s brief lists and summarizes the regulations and statutes to which it refers. CFC has found, in examining those statutes, that many would not apply to electric and gas utilities. None apply to energy consumption data. Other statutes, however, set a standard for implementation of Californians’ right to privacy under the state Constitution, particularly Civ. Code section 1798.80 *et seq.*<sup>30</sup> This statute imposes privacy standards which utilities, as businesses, are already required to meet.

Privacy statutes enacted in California understandably incorporate the public’s strong interest in maintaining the privacy of their information. Privacy statutes in California address the disclosure of information to third parties, and they are somewhat more protective than rules proposed by the Center for Democracy and Technology, as illustrated below.

The Information Practices Act of 1977 (Civ. Code sections 798 *et seq.*) defines a third party as “one or more of the following:

1. A business that is a separate legal entity from the business that has an established business relationship with a customer.

---

<sup>28</sup> MERCURYNEWS.COM: “Energy hearing draws litany of complaints about PG&E tactics” (Nov. 11, 2010). [http://www.mercurynews.com/breaking-news/ci\\_16584040?nclick\\_check=1](http://www.mercurynews.com/breaking-news/ci_16584040?nclick_check=1)

<sup>29</sup> *Id.*

<sup>30</sup> See e.g., Civ. Code §1798.1

2. A business that has access to a database that is shared among businesses, if the business is authorized to use the database for direct marketing purposes, unless the use of the database is exempt under [another section]
3. A business not affiliated by a common ownership or common corporate control with the business required to comply with [disclosure requirement].<sup>31</sup>

*CDT's corresponding definition is:*

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

Information included in the definition of personal information in privacy statutes is very specific:

- (i) Name and address;
- (ii) Electronic mail address;
- (iii) Age or date of birth;
- (iv) Names of children;
- (v) Electronic mail or other addresses of children;
- (vi) Number of children;
- (vii) The age or gender of children;
- (viii) Height;
- (ix) Weight;
- (x) Race;
- (xi) Political party affiliation;
- (xii) Medical condition;
- (xiii) Drugs, therapies, or medical products or equipment used, purchased, leased, or rented;
- (xiv) Real property purchased, leased, or rented;
- (xv) The kind of service provided;
- (xvi) Social security number;
- (xvii) Bank account number;
- (xviii) Credit card number;
- (xix) Debit card number;
- (xx) Bank or investment account, debit card, or credit card balance;
- (xxi) Payment history;
- (xxii) Information pertaining to the customer's credit-worthiness, assets, income, or liabilities.<sup>32</sup>

---

<sup>31</sup> Civil Code § 1798.83(a)

<sup>32</sup> Civ. Code §§ 1798.29(e); 1798.83(e)(6); Bus. & Prof. Code § 22577(a)

CDT rules define Covered Information as follows:

*Rule 1.(b) Covered Information. “Covered information” is any electrical or gas usage information when associated with any information that can reasonably be used to identify an individual, family, household, or residence, or non-residential customer, except that covered information does not include electrical or gas usage information from which identifying information has been removed such that an individual, family, household, or residence or non-residential customer cannot reasonably be identified or re-identified.*

Privacy standards incorporated in California statutes might be called “best practices” because they are practices prescribed by law. They may not be waived.<sup>33</sup> Standards for third party relationships incorporated in California privacy statutes are shown below, followed by CDT’s proposed rules in Italics: and CFC Comments.

1. A customer must be provided with a written summary of all his or her rights.<sup>34</sup>

*CDT Rule 2. (a) Generally. Covered entities shall provide customers with meaningful, clear, accurate, specific, and comprehensive notice regarding the collection, storage, use, and disclosure of covered information.*

CFC: It is unreasonable to expect utility customers to anticipate that information gathered to render invoices will be sold to marketers. Utility customers should be given notice of what information is being compiled and distributed by the utility, and what they can do to stop it.

2. Customer consent is required before any disclosures are made to a third party.<sup>35</sup>

*CDT Rule 6. USE AND DISCLOSURE LIMITATION*

*(a) Generally. Covered information shall be used solely for the purposes specified by the covered entity in accordance with section 3.*

*(b) Primary Purposes. An electric service provider, electrical corporation, gas corporation or community choice aggregator may collect, store and use covered information for primary purposes without customer consent.*<sup>36</sup> *Other covered*

---

<sup>33</sup> Civ Code § 1785.13;

<sup>34</sup> Civ. Code § 1785.11(d) & (e)

<sup>35</sup> Civ Code § 1786(12)(d) & (e); 1798.24; 1799.1; 1812.638(d); Cal. Ed. Code § 76222; 76242; Fin. Code § 4051.5(b); 4052.5; 4056(b)(2) Gov. Code § 11019.9; etc.

<sup>36</sup> Primary Purpose is defined as “(c) Primary Purposes. The “primary purposes” for the collection, storage, use or disclosure of covered information are to—

(1) provide or bill for electrical power or natural gas,  
(2) fulfill other operational needs of the electrical or natural gas system or grid,  
(3) provide services as required by state or federal law or specifically authorized by an

*entities may collect, store and use covered information only with prior customer consent, except as otherwise provided here*

*(d) Secondary Purposes. No covered entity shall use or disclose covered information for any secondary purpose without obtaining the customer's prior, express, written authorization for each such purpose, provided that authorization is not required when information is—*  
*(1) provided to a law enforcement agency in response to lawful process;*  
*(2) [required] [authorized] by the Commission pursuant to its jurisdiction and control*

**CFC:** An electric or gas corporation should not be deciding what information it will reveal to third parties. That choice should be left to consumers. Rules should be adopted which prohibit disclosure of non-public information unless the consumer agrees to its release. Where the consumer says, "No," the utility may appeal to the Commission for permission to release the data.

3. A business must undertake best efforts to ensure information released to third parties is accurate and secure, and keep a copy of what was released for further investigation.<sup>37</sup>

*CDT Rule 7. [Covered entities shall ensure that covered information they collect, store, use, and disclose is reasonably accurate and complete or otherwise compliant with applicable rules and tariffs regarding the quality of energy usage data.*

4. Limiting disclosure to certain specified people which are known to have an interest in the data and not just anyone.<sup>38</sup> For example, 1786.12(d) states ininvestigative reports may be prepared for employment purposes; as a factor in determining a consumer's eligibility for insurance or the rate for any insurance; or to determine the consumer's eligibility for a license or other benefit issued by the government; to provide support; or in connection with the hiring of a dwelling unit,

*CDT's Rule 6 attempts to limit recipients by describing primary and secondary purposes for which non-public information may be released.*

CFC: At least one category of primary purpose is much too broad. Information may be released to "fulfill other operational needs of the electrical or natural gas system or grid." The phrase "operational needs" is not defined and thus

---

order of the Commission, or

(4) implement demand response, energy management, or energy efficiency programs operated by, or on behalf of and under contract with, an electrical or gas corporation, electric service provider, or community choice aggregator.

Secondary Information is anything else.

<sup>37</sup> Civ. Code § 1785.14(b); Civ. Code§ 1786(11); Civ. Code § 1798.81;

<sup>38</sup> Civ. Code 1785.11(b); Civ Code § 1786(12)(d) & (e); Bus. & Prof. Code § 22575(b)

left to the discretion of the utility. Consumers' interest in keeping their personal information private is not sufficiently protected.

5. Disclosing the recipients of any customer data and all inquiries from third parties which were received in the previous twelve months (name, address, telephone number).<sup>39</sup>

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

*(2) each category of covered information that is disclosed to third parties [for a secondary purpose, or for a primary purpose under which the third party is providing services directly to customers], and, for each such category, (i) the purposes for which it is disclosed, and (ii) the identities of the third parties to which it is disclosed;*

6. Any 'business' must "require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information."<sup>40</sup>

*Rule 6(c). (1) Initial Disclosure by a Covered Entity. A covered entity may disclose covered information to a third party without customer consent for a primary purpose being carried out under contract with and on behalf of the entity disclosing the data, provided that the covered entity disclosing the data shall, by contract, require the third party to agree to collect, store, use, and disclose the covered information under policies, practices and notification requirements no less protective than those under which the covered entity itself operates as required under this rule and, if the information is being disclosed for demand response, energy management or energy efficiency purposes, the disclosing entity permits customers to opt out of such disclosure.*

7. When a business knows or reasonably should know that within the previous one year period a third party used the personal information of a customer for the third parties' direct marketing purposes, the business must, upon receipt of a request by a customer, disclose in writing or by e-mail:

- the category of information used<sup>41</sup>
- names and addresses of all third parties (and examples of the products or services marketed, if necessary) that received personal information for direct marketing purposes during the preceding calendar year.<sup>42</sup>

#### *CCDT Rule 8. . DATA SECURITY*

---

<sup>39</sup> Civ. Code 1785.10(d); 1786.10(c) Fin. Code § 4056

<sup>40</sup> Civil Code § 1798.81.5.(b); Fin. Code §§ 4053(b)(2)(C) & 4056(9)(b); Civ. Code § 1798.19.

<sup>41</sup> Civil Code § 1798.83(a)(1)

<sup>42</sup> Civil Code § 1798.83(a)

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

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

CFC: There is no apparent reason for withholding information about a breach in security procedures from the Commission. Notification to the Commission should occur simultaneously with notice to the customer.

8. A customer is entitled to notice of any breach of security which resulted in disclosure of personal information. Notice is to be given by e-mail, and posting of the notice on the business' web site, and sending the notice to major statewide media.<sup>43</sup>

*CDT Rule 8(b) , Upon request by the Commission, covered entities shall notify the Commission of security breaches of covered information.]*

CFC: There is no apparent reason for withholding information about a breach in security procedures from the Commission. Notification to the Commission should occur simultaneously with notice to the customer.

9. Every agency that provides an investigative report to a third person must "make a copy of that report available, upon request and proper identification, to the consumer for at least two years after the date that the report is provided to the other person.<sup>44</sup>

#### *4. INDIVIDUAL PARTICIPATION (ACCESS AND CONTROL)*

(a) *Access. Covered entities shall provide to customers upon request convenient and secure access to their covered information—*

*... (2) The Commission shall, by subsequent rule, prescribe what is a reasonable time for responding to customer requests for access.*<sup>45</sup>

CDT has addressed the elements of California's privacy legislation, but not in the same manner as California statutes. The Commission should adopt rules which mirror standards enacted by the legislature.

SDG&E and SoCal also argue "the extent of authority and jurisdiction bestowed upon the CPUC is measured by the specific constitutional or statutory origin from which

---

<sup>43</sup> Civil Code § 1798.82(a); 15 USC § 7001

<sup>44</sup> Civ. Code § 1786(11)

<sup>45</sup> Civil Code § 1798.84; Fin. Code § 4057

it derives its regulatory power. ... [T]he primary limiting factor on the Commission's authority and jurisdiction to regulate entities that are not public utilities may depend on whether the explicit power is 'cognate or germane' to the regulation of public utilities".<sup>46</sup> There can be no question that consumption data must be protected: "An electrical corporation or gas corporation 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."<sup>47</sup> It would defeat the purposes of the statute, and other privacy statutes, if third parties were able to take information from the utility and use it indiscriminately and without customer consent. Protection of consumption data is clearly cognate and germane to the Commission's supervision of public utilities.

The legislature has required that a utility releasing consumption data to a 3<sup>rd</sup> party 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."<sup>48</sup> They suggest that the Commission direct the utility to interrupt or cutoff the flow of utility information regarding a consumer's energy usage."<sup>49</sup> The legislature has appointed utilities, not the Commission, with the duty to withhold information from third parties when there is any suspicion that the third party will not protect it. If utilities would perform the duties given them by the Legislature, there would be no need for the Commission to exercise jurisdiction over third parties.

#### **D. EnerNoc, TechNet, Energy Control 14 Corporation & Tendril Networks**

EnerNoc *et al.* argue that "entities" subject to Commission jurisdiction must meet the statutory definitions for "public utility" (Public Utilities (PU) Code §216(a))" and, if they do not, they are not subject to Commission jurisdiction.<sup>50</sup> A court addressing the

---

<sup>46</sup> SDG&E/SoCal Gas Jurisdiction Br. at 4.

<sup>47</sup> Pub. Util. Code § 8380(d)

<sup>48</sup> Pub. Util. Code § 8380(e)(2)

<sup>49</sup> SDG&E/SoCal Jurisdiction Br at 7-8.

<sup>50</sup> EnerNoc *et al.* Jurisdiction Brief at 3.

same issue found, however, that the PUC’s jurisdiction is not limited to public utilities.<sup>51</sup> Arguments about whether EnerNoc *et al.* are public utilities are, therefore, irrelevant.

Their next argument is that there is no “legislative basis or rationale for Commission jurisdiction over such ‘entities’” because they are already “subject to a wide range of existing California law and oversight.”<sup>52</sup> The response is, as stated earlier, is that only the Commission has jurisdiction to safeguard electric and gas consumption data. Somewhat inconsistently, they also argue that there is no evidence that regulation of their activities is warranted and would create barriers to the expected efficiencies to be gained through the use of smart meters..<sup>53</sup>

California laws prohibiting discrimination have been on the books a long time, and federal laws even longer. It is unlikely that the legislature would deny customers of third parties the same privacy protections as customers of utilities. The right to privacy is Constitutionally derived. Any effect such privacy protections may have on “the expected efficiencies to be gained through the use of smart meters”<sup>54</sup> must be disregarded unless the two can be reconciled.

Another argument the businesses float is that “Section 8380 makes clear that the Commission is to focus and adopt rules limited to what the jurisdictional IOU can or cannot do with a customer’s data, . . . . This law does not seek to regulate either customers or “entities” with whom they consent to share their data.”<sup>55</sup> They appear to ignore section 8380(e)(2) which requires an IOU to impose rules by contract on third parties. The contract will require any third party 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, and prohibits the use of the data for a secondary commercial purpose . . . without the customer’s consent.”<sup>56</sup> Many other privacy statutes contain a similar provision.<sup>57</sup> The intervenors should be held to the same standard as other businesses.

---

<sup>51</sup> *PG&E v. PUC* (2004) 118 Cal. App. 4th 1174, 1198.

<sup>52</sup> EnerNoc *et al.* Jurisdiction Brief at 5.

<sup>53</sup> *Id.*

<sup>54</sup> EnerNoc *et al.* Jurisdiction Brief at 7.

<sup>55</sup> EnerNoc *et al.* Jurisdiction Brief at 8-9.

<sup>56</sup> Pub. Util. Code § 8380(e)(2)

<sup>57</sup> See, Civ. Code § 1785.14(b); Civ. Code§ 1786(11); Civ. Code § 1798.18; Civil Code § 1798.81.5.(b)

## II. CONCLUSION

The legislature has recognized energy consumption data is revealing and its disclosure should be limited. A ruling that the Commission does not have jurisdiction over third parties might be issued if utilities were willing to assume the role intended by the legislature in Pub. Util. Code section 8380. If, however, the utilities are not required to monitor the use of data they have supplied to a third party, then the Commission has sufficient legal basis to assert jurisdiction over third parties acting in an area cognate and germane to utility regulation.

Dated: December 6, 2010

Respectfully submitted,

CONSUMER FEDERATION OF CALIFORNIA

By: \_\_\_\_\_ //s//  
Alexis K. Wodtke

Consumer Federation of California  
520 S. El Camino Real, Suite 340  
San Mateo, CA 94402  
Phone: (650) 375-7847  
Fax: (650) 343-1238  
Email: [lex@consumercal.org](mailto:lex@consumercal.org)

## APPENDIX A

### California State & Federal Consumer Privacy Protection Laws

Civil Code §§ 1785.1 - 1785.36 applies only to consumer credit reporting agencies, and not to utilities. It does however provide useful guidelines for the Commission to adopt, e.g.,

- Creates a right of people to inspect information held by the agency
- Requires the agency to disclose the recipients of any consumer credit report within the previous two years (name, address, telephone number)
- Requires the agency to disclose all inquiries it received in the previous twelve months about a consumer's credit transaction (name, address, telephone number)
- Limits an agency's release of a consumer credit report to situations in which credit is offered by a lender (not sought by a customer) and the customer has agreed to allow his/her name to be used
- Limits an agency's release of a consumer credit report to certain circumstances, e.g., in connection with a credit transaction, employment request, insurance application or claim, home rental application, license application, other demonstrated business need, or where disclosure to a government agency is required by law.
- Limits the information to be released to the name and address of the consumer and only where the customer has not requested that his/her name be withheld ("security alert") or that no credit report be issued ("security freeze")
- Requires the agency to "follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates, and to keep a copy of what was released for further investigation
- Providing a customer with a written summary of all rights the consumer has in a form substantially similar to the notice in Civil Code section 1785.15(f)23.

**Civ. Code §§ 1786 et seq.**, the Investigative Consumer Reporting Agencies Act , applies to investigative reporting agencies which are collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating consumer information needed by insurance companies, employers, property owners, courts, etc.<sup>58</sup> The consumer must be given access to all files maintained by the agency with the exception of the non-public source of the information.<sup>59</sup> "The investigative consumer reporting agency shall also:

- disclose to the customer the dates, original payees, and amounts of any checks or charges upon which is based any adverse characterization of the consumer."<sup>60</sup>
- identify each recipient of an investigative report during the previous three years, by name or trade name, and address & telephone, if requested.

---

<sup>58</sup> Civ. Code § 1786

<sup>59</sup> Civ. Code § 1786(3)

<sup>60</sup> Civ. Code § 1786(10)(e)

The class of persons to whom an agency is permitted to provide a report, with the customer's consent, is limited to prospective employers, a court, and a person who it has reason to believe will use the information:

- for employment purposes,
- to determine whether a customer is eligible for insurance or rate for that insurance,
- whether a customer has the qualifications to obtain a license or other benefit from the government,
- to accompany a judge's support order against the consumer, or for the rental of property.<sup>61</sup>

The report may not contain medical information unless the consumer agrees.<sup>62</sup> Every agency that provides an investigative report to a third person must "make a copy of that report available, upon request and proper identification, to the consumer for at least two years after the date that the report is provided to the other person."<sup>63</sup>

**California Civil Code §§ 1798 et seq.** (Information Practices Act of 1977), was adopted to provide greater protection for the constitutional right to privacy "threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies and the increasing use of computers and other sophisticated information technology."<sup>64</sup> It directs agencies of the state to maintain "only personal information which is relevant and necessary to accomplish a purpose of the agency required or authorized by the California Constitution or statute or mandated by the federal government."

The statute defines "personal information" as "any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual."

All records are to be maintained, "to the maximum extent possible, with accuracy, relevance, timeliness, and completeness."<sup>65</sup> The statute directs agencies to record the source of information it gathers<sup>66</sup> and, where possible, obtain the information directly from the individual it is about..<sup>67</sup> Agencies are directed to "establish rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing personal information" to include "any other rules and procedures adopted pursuant to this chapter and the remedies and penalties for noncompliance."<sup>68</sup>

---

<sup>61</sup> Civ Code § 1786(12)(d) & (e).

<sup>62</sup> Civ Code § 1786(12)(f)

<sup>63</sup> Civ. Code§ 1786(11)

<sup>64</sup> Civ. Code §1798.1.

<sup>65</sup> Civ. Code § 1798.18.

<sup>66</sup> Civ. Code § 1798.16.

<sup>67</sup> Civ. Code § 1798.15

<sup>68</sup> Civ. Code § 1798.20.

Any contractor who will receive information in the course of its performance of an agency function must agree that it will comply with the requirements of chapter 1798.<sup>69</sup>

**Civil Code §§ 1798.80 – 1798.84** applies to IOUs. As regulated entities, they would be exempt only if the business “is regulated by state or federal law providing greater protection to personal information than that provided by this section.”<sup>70</sup> A “business” is defined in part as follows: “Business” means a ... corporation ... or other group, however organized and whether or not organized to operate at a profit, ...<sup>71</sup> Section 1798.81.5 sets the standards to be met by a business in the area of privacy.

1798.81.5. (a) It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own or license personal information about Californians to provide reasonable security for that information.

*Security Procedures and Practices.* A business is required 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.
- shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information.<sup>72</sup>

*Personal information* is defined to include:

- Social security number.
- Driver's license number or California identification card number.
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
- Medical information defined as any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.<sup>73</sup>

*Notice of breach.* A business with computerized data that includes personal information shall:

- disclose any breach of the security of the system<sup>74</sup> following discovery or notification ... to any resident of California whose unencrypted personal

---

<sup>69</sup> Civ. Code § 1798.19

<sup>70</sup> Civil Code § 1798.81.5(e)(5)

<sup>71</sup> Civil Code § 1798.80(a)

<sup>72</sup> Civil Code § 1798.81.5.(b)

<sup>73</sup> Civil Code § 1798.81.5(d). A broader definition of personal information is adopted in the statute related to third party marketing of personal information. Civil Code § 1798.83(e)(7).

<sup>74</sup> (d) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Civil Code § 1798.82. (d)

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, . . . .

- notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, . . . .<sup>75</sup>

Notice is to be given by electronic service if it conforms to a federal law<sup>76</sup> setting standards for electronic service. If not, notice is to be given, instead, by e-mail, and posting of the notice on the business' web site, and sending the notice to major statewide media

*Third party marketing.* If a business that "has an established business relationship with a customer and within the immediately preceding calendar year has disclosed personal information to third parties, . . . knows or reasonably should know that the third parties used the personal information for the third parties' direct marketing purposes, the business must, upon receipt of a request by a customer, disclose in writing or by e-mail:

- the category of information used<sup>77</sup>
- the names and addresses of all third parties (and examples of the products or services marketed, if necessary) that received personal information for direct marketing purposes during the preceding calendar year.<sup>78</sup>

A business can avoid the disclosure if it adopts a policy of not disclosing personal information of customers to third parties... unless the customer first affirmatively agrees (or opts in) to that disclosure: notifies the customer of his or her right to prevent disclosure of personal information; and provide[s] the customer with a cost-free means to exercise that right."<sup>79</sup>

"*Third party*" is defined as "one or more of the following:

- A business that is a separate legal entity from the business that has an established business relationship with a customer.
- A business that has access to a database that is shared among businesses, if the business is authorized to use the database for direct marketing purposes, unless the use of the database is exempt under [another section]

---

<sup>75</sup> Civil Code § 1798.82. (a)

<sup>76</sup> 15 USC § 7001.

<sup>77</sup> The following categories of information must be identified: (i) Name and address; (ii) Electronic mail address; (iii) Age or date of birth; (iv) Names of children; (v) Electronic mail or other addresses of children; (vi) Number of children; (vii) The age or gender of children; (viii) Height; (ix) Weight; (x) Race; (xv) Political party affiliation; (xvi) Medical condition; (xvii) Drugs, therapies, or medical products or equipment used; (xviii) The kind of product the customer purchased, leased, or rented; (xix) Real property purchased, leased, or rented; (xx) The kind of service provided; (xxi) Social security number; (xxii) Bank account number; (xxiii) Credit card number; (xxiv) Debit card number; (xxv) Bank or investment account, debit card, or credit card balance; (xxvi) Payment history; (xxvii) Information pertaining to the customer's creditworthiness, assets, income, or liabilities. Civ, Code § 1798.83(e)(6).

<sup>78</sup> Civil Code § 1798.83(a)

<sup>79</sup> Civil Code § 1798.83(c)(2)

- A business not affiliated by a common ownership or common corporate control with the business required to comply with [disclosure requirement].<sup>80</sup>

Third-party affiliates that share the same brand name are also subject to disclosure requirements.<sup>81</sup>

*Waiver.* None of the statutory requirements can be waived, but a business which has not made a complete disclosure in compliance with the statute is permitted to claim, as a complete defense, that within 90 days after the omission is discovered, it provides all of the necessary information; the withholding may not, however, be “willful, intentional, or reckless.”

*Civil Penalties.* If a customer is injured by a business’ failure to keep personal information secure as specified in the statute, the customer may claim damages and civil penalties of \$500 per violation. If the business’ violation of the third party disclosure law was “willful, intentional, or reckless,” the penalty is \$3,000 per violation.<sup>82</sup>

**Civil Code §§ 1798.85-1798.86** is applicable to any a person or entity and prohibits specific types of disclosure of an individual’s social security number. Any waiver of the specific prohibitions against disclosure is void and unenforceable. The statute provides that no person or entity may:

- Intentionally communicate or otherwise make available to the general public an individual’s social security number
- Print an individual’s social security number on any card used to access products or services they provide.
- “Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.”
- “Require an individual “to use his or her social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site.”
- “Print an individual’s social security number on any materials that are mailed to the individual, unless the document on which the SS# is printed is mailed in an envelope and the document is “part of an application or enrollment process, or [used] to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the social security number.””
- “Encode or embed a social security number in or on a card or document, including, but not limited to, using a barcode, chip, magnetic strip, or other technology, in place of removing the social security number.”<sup>83</sup>

**Financial Code §§ 4050-4060** applies to financial institutions, not utilities. A financial institution is defined as “any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 of the United States Code and

<sup>80</sup> Civil Code § 1798.83(a)

<sup>81</sup> Civil Code § 1798.83(a)

<sup>82</sup> Civil Code § 1798.84; Fin. Code § 4056

<sup>83</sup> Civ. Code § 1798.8(5)

doing business in this state. An institution that is not significantly engaged in financial activities is not a financial institution.<sup>84</sup> The federal statute referenced identifies specific activities which are financial<sup>85</sup> and identifies a number of factors to be considered when deciding whether an institution should be considered a “financial institution.”<sup>86</sup> Utilities are not in the business of banking, insuring, underwriting or other activities identified in the statute..

The California Financial Privacy Act was enacted to fill in the interstices of federal financial legislation after passage of the Gramm-Leach-Bliley Act. Its purpose is to require financial institutions “to provide their consumers notice and meaningful choice about how consumers' nonpublic personal information is shared or sold by their financial institutions” and “to afford persons greater privacy protections than those provided in ... the federal Gramm-Leach-Bliley Act, ...<sup>87</sup>

The requirements of the Financial Privacy Act are similar to other privacy statutes.

- It prohibits disclosure of ‘personal information’ without customer consent and, in the case of affiliates, prohibits disclosure if the customer asks that the information be kept private.<sup>88</sup>
- Where disclosure to a third party is permitted, as in a joint offering of a financial product, a written agreement between the parties that the nonpublic personal information will remain confidential and will not be disclosed except in connection with the joint financial offering.
- A third party who receives non-public personal information is bound by all of the statutory prohibitions applicable to the original holder of the information

If there is a negligent disclosure of nonpublic personal information in violation of the statute, the financial institution “shall be liable, irrespective of the amount of damages suffered by the consumer as a result of that violation, for a civil penalty not to exceed \$2,500 per violation or, if information of more than one individual is disclosed, \$500,000.<sup>89</sup> The action for recovery of the penalty may be brought either by the attorney or the agency that regulates the financial institution.

**15 U.S.C. §§ 6801-6809** is the Gramm-Leach-Bliley Act which the California legislature believed did not provide adequate protection.

**Gov. Code 11549.5** describes the functions to be served by the Office of Privacy Protection. The Office “inform[s] the public”, “make[s] recommendations to organizations,” and “promote[s] voluntary and mutually agreed upon nonbinding

---

<sup>84</sup> Fin. Code § 4052(c)

<sup>85</sup> 12 USC 1843(k)(4) identifies specific financial activities including **(A)** Lending, exchanging, transferring, investing for others, or safeguarding money or securities; **(B)** Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, and acting as principal, agent, or broker for purposes of the foregoing, in any State; **(C)** Providing financial, investment, or economic advisory services, including advising an investment company ; **(D)** Issuing or selling instruments representing interests in pools of assets permissible for a bank to hold directly; **(E)** Underwriting, dealing in, or making a market in securities; **(F)** Engaging in any activity that the Board has determined, by order or regulation that is in effect on November 12, 1999, to be so closely related to banking or managing or controlling banks as to be a proper incident thereto ... ”

<sup>86</sup> 12 USC 1843(K)(3)

<sup>87</sup> Fin. Code § 4051.

<sup>88</sup> Fin. Code § 4052.5

<sup>89</sup> Fin. Code § 4056

arbitration and mediation,” relating to privacy. The Office receives individuals’ complaints; helps consumers handle complaints and investigates and prosecutes ‘privacy-related crimes.’ The Office trains and acts in coordination with “local, state, and federal law enforcement agencies.”

The Commission’s rules would establish a standard of conduct for the utilities. Section 11549.5 simply allows the Office of Privacy Protection to help customers aggrieved by a business’ actions.

**Bus. & Prof. Code §§ 22575-22579** apply to “[a]n operator of a commercial Web site or online service” that collects through the web site personally identifiable information of Californians.<sup>90</sup> This statute presumably applies to utilities and preempts any other law or regulation.<sup>91</sup> “Personally identifiable information” is defined to include:

- (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.
- (6) Any other identifier that permits the physical or online contacting of a specific individual.<sup>92</sup>

The web site operator must “conspicuously post” its privacy policy on its Web site, by creating a Web page where it is posted which must be” the homepage or first significant page after entering the Web site. As alternatives, it may post an icon with a link to the private policy web page in the same places. The icon must contain the word privacy and in a color which contrasts with the color of the web page. A text link may substitute for an icon, but it must be written in capital letters and use a font bigger than surrounding text or in contrasting type, font or color so as to stand out from surrounding text.<sup>93</sup> An online service may use “any other reasonably accessible means of making the privacy policy available for consumers of the online service.”<sup>94</sup>

The privacy policy of the web operator must

- “[i]dentify the categories of personally identifiable information that the operator collects,”
- the categories of third-party persons or entities with whom the operator may share that information.
- Describe any process available to a user or visitor of a web site to review and request changes to any of his or her personal information
- Describe the process by which the operator notifies consumers of material changes to the privacy policy
- Identify the effective date of the policy.<sup>95</sup>

---

<sup>90</sup> Bus. & Prof. Code § 22577(b)(5)

<sup>91</sup> Bus. & Prof. Code § 22578

<sup>92</sup> Bus. & Prof. Code § 22577(a)

<sup>93</sup> Bus. & Prof. Code § 22575(b)

<sup>94</sup> Bus. & Prof. Code § 22575(b)

<sup>95</sup> Bus. & Prof. Code § 22575(b)

**18 U.S. Code § 1028** (Federal Identity Theft Assumption and Deterrence Act of 1998) establish penalties for certain crimes related to the theft of an individual's identity. The crimes include:

- producing a false identification document
- transferring a false identification document knowing that such document or feature was stolen or produced without lawful authority
- possesses with intent to use unlawfully or transfer unlawfully five or more identification documents
- Knowingly possesses a false identification document with intent to defraud the United States;
- knowingly produces, transfers, or possesses a tool used to make false documents with the intent to produce a false identification document
- knowingly possesses an identification document or
- authentication feature of the United States which is known to be stolen or produced without lawful authority knowing
- unlawfully and knowingly transfers, possesses, or uses a means of identification of another person with the intent to violate federal or state law
- knowingly traffics in false or actual authentication features for use in false identification documents or tools

**Public Utilities Code §§ 8380 -8381**

Chapter 497, Statutes of 2010

Senate Bill No. 1476

Information obtained from a customer must be kept confidential by IOU electric and gas utilities ("IOU's). Public Utilities Code § 8380(b)(1) (SB 1476) makes usage data confidential: "An electrical corporation or gas corporation shall not share, disclose, or otherwise make accessible to any third party a customer's electrical or gas consumption data, except as provided in subdivision (e) or upon the consent of the customer."

Subdivision (e) allows disclosure under three sets of circumstances:

- all information has been removed regarding the individual identity of a customer;
- for system, grid, or operational needs, or the implementation of demand response, energy management, or energy efficiency programs, provided that, for contracts entered into after January 1, 2011, the utility has required 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; or
- as required or permitted under state or federal law or by an order of the commission.

A third party is bound by the terms of its agreement with the IOU to keep personal information of customers, including consumption data, private and secure.

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

Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's own Motion to Actively Guide Policy in California's Development of a Smart Grid System.

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

**CERTIFICATE OF SERVICE**

I hereby certify that on December 6, 2010, I served on all parties on the service list for R.09-02-019, by email, true copies of the original of the following documents which are attached hereto:

**REPLY BRIEF OF THE CONSUMER FEDERATION OF CALIFORNIA  
CONCERNING THE COMMISSION'S AUTHORITY  
OVER RECIPIENTS OF CONSUMER USAGE DATA.**

The e-mail addresses to which these documents were sent are shown on an attachment.

Dated: December 6, 2010, at San Mateo, CA.

## CONSUMER FEDERATION OF CALIFORNIA

//s//  
Alexis K. Wodtke  
Consumer Federation of California  
520 S. El Camino Real, Suite 340  
San Mateo, CA 94402  
Phone: (650) 375-7847  
Fax: (650) 343-1238  
Email: [lex@consumercal.org](mailto:lex@consumercal.org)

Service List for R.08-12-009 (Smart Grid):

MARTIN	HOMECA	martinhomedc@gmail.com
CARL	GUSTIN	carlgustin@groundedpower.com
VLADIMIR	OKSMAN	vladimir.oksman@lantiq.com
JOSEPH	ANDERSEN	jandersen@tiaonline.org
JEFF	CAMPBELL	jeffrcam@cisco.com
JIM	HALPERT, ESQ	jhalpert@dlapiper.com
DEAN R.	BRENNER	dbrenner@qualcomm.com
JULES	POLONETSKY	julespol@futureofprivacy.org
LILLIE	CONEY	coney@epic.org
MICHAEL	SACHSE	michael.sachse@opower.com
CAMERON	BROOKS	cbrooks@tendrilinc.com
STEVEN D.	PATRICK	SDPatrick@SempraUtilities.com
NORMAN A.	PEDERSEN	npedersen@hanmor.com
STEVEN G.	LINS	slins@ci.glendale.ca.us
DANIEL W.	DOUGLASS	douglass@energyattorney.com
XAVIER	BALDWIN	xbaldwin@ci.burbank.ca.us
KRIS G.	VYAS	kris.vyas@sce.com
ALLEN K.	TRIAL	ATrial@SempraUtilities.com
LEE	BURDICK	lburdick@higgslaw.com
DONALD C.	LIDDELL	liddell@energyattorney.com
MICHAEL	SHAMES	mshames@ucan.org
CHARLES R.	TOCA	ctoca@utility-savings.com
ROBERT	SMITH, PH.D.	bobsmithtl@gmail.com
MONA	TIERNEY-LLOYD	mtierney-lloyd@enernoc.com
EDWARD G.	CAZALET	ed@megawattsf.com
MICHAEL	TERRELL	mterrell@google.com
MARC D.	JOSEPH	mdjoseph@adamsbroadwell.com
COLLIN	BREAKSTONE	cbreakstone@control4.com
ELAINE M.	DUNCAN	elaine.duncan@verizon.com
FIELD	PICKERING	pickering@energyhub.net
MARGARITA	GUTIERREZ	margarita.gutierrez@sfgov.org
Lisa-Marie	Salvacion	lms@cpuc.ca.gov
FRASER D.	SMITH	fsmith@sfwater.org
SANDRA	ROVETTI	srovetti@sfwater.org
THERESA	BURKE	tburke@sfwater.org
MARCEL	HAWIGER	marcel@turn.org
MARTY	KURTOVICH	mkurtovich@chevron.com
CHRISTOPHER J.	WARNER	cjw5@pge.com
DAVID P.	DISCHER	david.discher@att.com
NORA	SHERIFF	nes@a-klaw.com
HAROLD	GALICER	harold@seakayinc.org
PETER A.	CASCIATO	pcasciato@sbcglobal.net
STEVEN	MOSS	steven@sfpower.org
LEE	TIEN	tien@eff.org
JEANNE B.	ARMSTRONG	jarmstrong@goodinmacbride.com
MARLO A.	GO	mgo@goodinmacbride.com
MICHAEL B.	DAY	mday@goodinmacbride.com

SARA STECK	MYERS	ssmyers@worldnet.att.net
JUDITH	SCHWARTZ	judith@tothept.com
ALEXIS K.	WODTKE	lex@consumercal.org
FARROKH	ALUYEK, PH.D.	farrokh.albuyeh@oati.net
MICHAEL	ROCHMAN	Service@spurr.org
MARK	SCHAEFFER	Mark.Schaeffer@granitekey.com
WILLIAM H.	BOOTH	wbooth@booth-law.com
JODY	LONDON	jody_london_consulting@earthlink.net
LEN	CANTY	lencanty@blackeconomiccouncil.org
JOSEPH F.	WIEDMAN	jwiedman@keyesandfox.com
KEVIN T.	FOX	kfox@keyesandfox.com
GREGG	MORRIS	gmorris@emf.net
ROBERT	GINAIZDA	robertginaizda@gmail.com
ENRIQUE	GALLARDO	enriqueg@greenlining.org
AARON J.	BURSTEIN	aaron.burstein@gmail.com
DEIRDRE K.	MULLIGAN	dkm@ischool.berkeley.edu
JENNIFER	LYNCH	jlynch@law.berkeley.edu
JENNIFER M.	URBAN	jurban@law.berkeley.edu
MIKE	TIERNEY	kerry.hattevik@nrgenergy.com
RICH	QUATTRINI	rquattrini@energyconnectinc.com
MICHAEL	WEISSMAN	michael_w@copper-gate.com
DIANA	POLULYAKH	diana@aspectlabs.com
TODD S.	GLASSEY	TGlassey@Certichron.com
STEVE	BOYD	seboyd@tid.org
DAVID	ZLOTLOW	dzlotlow@caiso.com
DENNIS	DE CUIR	dennis@ddecuir.com
SCOTT	TOMASHEFSKY	scott.tomashefsky@ncpa.com
JIM	HAWLEY	jhawley@technet.org
LAUREN	NAVARRO	Inavarro@edf.org
LESLA	LEHTONEN	Lesla@calcable.org
CHASE B.	KAPPEL	cbk@eslawfirm.com
MICHAEL	COOP	mcoop@homegridforum.org
CASSANDRA	SWEET	cassandra.sweet@dowjones.com
DAVID J.	BLACKBURN	dblackburn@caiso.com
GREY	STAPLES	gstaples@mendotagroup.net
JANICE	LIN	jlin@strategen.com
RYN	HAMILTON	ryn@rynhamiltonconsulting.com
STEPHANIE C.	CHEN	stephaniec@greenlining.org
TAM	HUNT	tam.hunt@gmail.com
TIMOTHY N.	TUTT	ttutt@smud.org
ERIN	GRIZARD	EGrizard@deweysquare.com
JON	FORTUNE	jon.fortune@energycenter.org
MARTIN	HOMEC	martinhomec@gmail.com
MICHAEL	O'KEEFE	mokeefe@efficiencycouncil.org
RICHARD W.	RAUSHENBUSH	r.raushenbush@comcast.net
SEPHRA A.	NINOW	sephra.ninow@energycenter.org
SUE	MARA	sue.mara@rtoadvisors.com kladko@aspectlabs.com ep@aspectlabs.com

JOHN	QUEALY	john.quealy@canaccordadams.com
MARK	SIGAL	mark.sigal@canaccordadams.com
BARBARA R.	ALEXANDER	barbalex@ctel.net
CHRISTOPHER	JOHNSON	crjohnson@lge.com
SHELLEY-ANN	MAYE	smaye@nappartners.com
JULIEN	DUMOULIN-SMITH	julien.dumoulin-smith@ubs.com
KEVIN	ANDERSON	
MARIE	PIENIAZEK	mpieniazek@drenergyconsulting.com
WILLIAM	CHEN, ESQ.	wchen@ecsgrid.com
DAVID	RUBIN	david.rubin@troutmansanders.com
JENNIFER	SANFORD	jennsanf@cisco.com
MARY	BROWN	marybrow@cisco.com
JACKIE	MCCARTHY	jmccarthy@ctia.org
JAY	BIRNBAUM	jay.birnbaum@currentgroup.com
MATT	MCCAFFREE	
PUJA	DEVERAKONDA	puja@opower.com
ROBERT C.	ROWE	bob.rowe@northwestern.com
MONICA	MERINO	monica.merino@comed.com
STEPHEN	THIEL	sthiel@us.ibm.com
ANN	JOHNSON	ann.johnson@verizon.com
ED	MAY	ed.may@itron.com
RAYMOND	GIFFORD	rgifford@wbklaw.com
JIM	SUEUGA	
PHIL	JACKSON	
LEILANI		
JOHNSON	KOWAL	leilani.johnson@ladwp.com
GREGORY	HEALY	GHealy@SempraUtilities.com
JORGE	CORRALEJO	jorgecorralejo@sbcglobal.net
DAVID	SCHNEIDER	dschneider@lumesource.com
LILY M.	MITCHELL	lmitchell@hanmor.com
DAVID	NEMTZOW	david@nemtzow.com
CRAIG	KUENNEN	ckuennen@ci.glendale.us
MARK S.	MARTINEZ	mark.s.martinez@sce.com
CASE	ADMINISTRATION	case.admin@sce.com
JANET	COMBS	janet.combs@sce.com
MICHAEL A.	BACKSTROM	michael.backstrom@sce.com
NGUYEN	QUAN	nquan@gswater.com
JEFF	COX	Jcox@fce.com
ESTHER	NORTHRUP	esther.northrup@cox.com
KELLY M.	FOLEY	KFoley@SempraUtilities.com
MIKE	SCOTT	mike@ucan.org
KIM	KIENER	kmkiener@cox.net
DONALD J.	SULLIVAN	djsulliv@qualcomm.com
HANNON	RASOOL	HRasool@SempraUtilities.com
TODD	CAHILL	TCahill@SempraUtilities.com
CAROL	MANSON	CManson@SempraUtilities.com
DESPINA	NIEHAUS	DNiehaus@SempraUtilities.com
CENTRAL	FILES	CentralFiles@SempraUtilities.com
JERRY	MELCHER	jerry@enernex.com
TRACEY L.	DRABANT	traceydrabant@bves.com

PETER T.	PEARSON	peter.pearson@bves.com
DAVID X.	KOLK	dkolk@compenergy.com
EVELYN	KAHL	ek@a-klaw.com
RICK	BOLAND	rboland@e-radioinc.com
JUAN	OTERO	juan.otero@trilliantinc.com
SHARON	TALBOTT	stalbott@control4.com
FARAMARZ	MAGHSOODLOU	faramarz@ieee.org
RUDY	REYES	rudy.reyes@verizon.com
AMANDA	WALLACE	mandywallace@gmail.com
NORMAN J.	FURUTA	norman.furuta@navy.mil
KRISTIN	GRENFELL	kgrenfell@nrdc.org
NINA	SUETAKE	nsuetake@turn.org
ROBERT	FINKELSTEIN	bfinkelstein@turn.org
MICHAEL E.	CARBOY	mcarboy@signalhill.com
ANDREW	MEIMAN	andrew_meiman@newcomb.cc
CASE	COORDINATION	regrelcpuccases@pge.com
DAVID	BAYLESS	dpb5@pge.com
DIONNE	ADAMS	DNG6@pge.com
KAREN	TERRANOVA	filings@a-klaw.com
KIMBERLY C.	JONES	Kcj5@pge.com
MICHAEL P.	ALCANTAR	mpa@a-klaw.com
MICHELLE	CHOO	micelle.choo@att.com
RICHARD H.	COUNIHAN	rcounihan@enernoc.com
SEEMA	SRINIVASAN	sls@a-klaw.com
STEPHANIE E.	HOLLAND	Stephanie.Holland@ATT.com
STEPHEN J.	CALLAHAN	stephen.j.callahan@us.ibm.com
TERRY	FRY	tmfry@nexant.com
MARGARET L.	TOBIAS	info@tobiaslo.com
BENJAMIN J.	KALLO	BKallo@rwbaird.com
BRIAN T.	CRAGG	bcragg@goodinmacbride.com
BRYCE	DILLE	bdille@jmpsecurities.com
JANINE L.	SCANCARELLI	jscancarelli@crowell.com
JEFFREY	SINSHEIMER	jas@cpdb.com
JOSHUA	DAVIDSON	joshdavidson@dwt.com
NORENE	LEW	nml@cpdb.com
SALLE E.	YOO	salleyoo@dwt.com
STEVE	HILTON	SDHilton@stoel.com
SUZANNE	TOLLER	suzannetoller@dwt.com
DAVID L.	HUARD	dhuard@manatt.com
MARIA	CARBONE	mariacarbone@dwt.com
DIANE I.	FELLMAN	Diane.Fellman@nrgenergy.com cem@newsdata.com
LISA	WEINZIMER	lisa_weinzimer@platts.com
PAUL	PRUDHOMME	prp1@pge.com
ROBERT	GNAIZDA	RobertGnaizda@gmail.com
ANGELA	CHUANG	achuang@epri.com
CARYN	LAI	caryn.lai@bingham.com
MEGAN	KUIZE	
ELLEN	PETRILL	epetrill@epri.com
ALI	IPAKCHI	ali.ipakchi@oati.com

CHRIS	KING	chris@emeter.com
JOHN	DUTCHER	ralf1241a@cs.com
JOHN	GUTIERREZ	john_gutierrez@cable.comcast.com
MIKE	AHMADI	mike.ahmadi@Granitekey.com
UZMA	ALMAKKY	uzma@crve.org
SEAN P.	BEATTY	sean.beatty@mirant.com
THOMAS W.	LEWIS	lewis3000us@gmail.com
DOUG	GARRETT	Douglas.Garrett@cox.com
BOB	STUART	rstuart@brightsourceenergy.com
NELLIE	TONG	nellie.tong@us.kema.com
VALERIE	RICHARDSON	Valerie.Richardson@us.kema.com
DOCKET	COORDINATOR	cpucdockets@keyesandfox.com
DAVID	MARCUS	dmarcus2@sbcglobal.net
REED V.	SCHMIDT	rschmidt@bartlewells.com
SAMUEL S.	KANG	samuelk@greenlining.org
STEVE	KROMER	jskromer@qmail.com
JENNIFER	URBAN	jurban@law.berkeley.edu
KINGSTON	COLE	kco@kingstoncole.com
PHILLIP	MULLER	philm@scdenergy.com
JANET	PETERSON	j_peterson@ourhomespaces.com
JOSEPH	WEISS	joe.weiss@realtimeacs.com
MICHAEL E.	BOYD	michaelboyd@sbcglobal.net
BARRY F.	MCCARTHY	bmcc@mccarthylaw.com
C. SUSIE	BERLIN	sberlin@mccarthylaw.com
MARY	TUCKER	mary.tucker@sanjoseca.gov
TOM	KIMBALL	tomk@mid.org
JOY A.	WARREN	joyw@mid.org
DAVID	KATES	
BARBARA R.	BARKOVICH	brbarkovich@earthlink.net
GAYATRI	SCHILBERG	gayatri@jbsenergy.com
DOUGLAS M.	GRANDY, P.E.	dgrandy@caonsitegen.com
DAVID E.	MORSE	davidmorse9@gmail.com
ANTHONY	E-RECIPIENT	e-recipient@caiso.com
HEATHER	IVANCOVICH	aivancovich@caiso.com
JOHN	SANDERS	hsanders@caiso.com
WAYNE	GOODIN	jgoodin@caiso.com
CAROLYN	AMER	wamer@kirkwood.com
TOM	KEHREIN	cmkehrein@ems-ca.com
BRIAN	POMALES	tpomales@arb.ca.gov
DANIELLE	THEAKER	brian.theaker@dynegy.com
DAVID L.	OSBORN-MILLS	danielle@ceert.org
JAMES	MODISSETTE	dave@ppallc.com
JAN	FINE	jfine@edf.org
JOHN	MCFARLAND	jmcfarland@treasurer.ca.gov
KELLIE	SHEARS	shears@ceert.org
LINDA	SMITH	kellie.smith@sen.ca.gov
RICHELLE	KELLY	lkelly@energy.state.ca.us
STEVEN A.	ORLANDO	ro@calcable.org
PRAMOD P.	LIPMAN	steven@lipmanconsulting.com
	KULKARNI	pkulkarni@energy.state.ca.us

LYNN	HAUG	lmh@eslawfirm.com
ANDREW B.	BROWN	abb@eslawfirm.com
BRIAN S.	BIERING	bsb@eslawfirm.com
GREGGORY L.	WHEATLAND	glw@eslawfirm.com
JIM	PARKS	jparks@smud.org
LOURDES	JIMENEZ-PRICE	lJimene@smud.org
VICKY	ZAVATTERO	vzavatt@smud.org
VIKKI	WOOD	vwood@smud.org
DAN	MOOY	dan.mooy@ventyx.com
KAREN		
NORENE	MILLS	kmills@cfbf.com
ROGER	LEVY	rogerl47@aol.com
JESSICA	NELSON	
JACK	ELLIS	jellis@resero.com
MICHAEL	JUNG	michael.jung@silverspringnet.com
ANNIE	STANGE	sas@a-klaw.com
MIKE	CADE	wmc@a-klaw.com
BENJAMIN	SCHUMAN	bschuman@pacific-crest.com
SHARON K.	NOELL	sharon.noell@pgn.com
TED	HOWARD	TRH@cpuc.ca.gov
Adam	Langton	ahl@cpuc.ca.gov
Aloke	Gupta	ag2@cpuc.ca.gov
Andrew	Campbell	agc@cpuc.ca.gov
Anthony	Mazy	am1@cpuc.ca.gov
Christopher R	Villarreal	crv@cpuc.ca.gov
Damon A.	Franz	df1@cpuc.ca.gov
David	Peck	dbp@cpuc.ca.gov
Farzad	Ghazzagh	fxg@cpuc.ca.gov
Gretchen T.	Dumas	gtd@cpuc.ca.gov
Jake	Wise	jw2@cpuc.ca.gov
Joyce	de Rossett	jdr@cpuc.ca.gov
Julie	Halligan	jmh@cpuc.ca.gov
Karin M.	Hieta	kar@cpuc.ca.gov
Lana	Tran	ltt@cpuc.ca.gov
Lauren	Saine	lbs@cpuc.ca.gov
Laurence	Chaset	lau@cpuc.ca.gov
Marzia	Zafar	zaf@cpuc.ca.gov
Matthew	Deal	mjd@cpuc.ca.gov
Max	Gomberg	mzx@cpuc.ca.gov
Michael B.	Pierce	mbp@cpuc.ca.gov
Michael	Colvin	mc3@cpuc.ca.gov
Rebecca	Tsai-Wei Lee	wtr@cpuc.ca.gov
Risa	Hernandez	rhh@cpuc.ca.gov
Sarah R.	Thomas	srt@cpuc.ca.gov
Steve	Roscow	scr@cpuc.ca.gov
Timothy J.	Sullivan	tjs@cpuc.ca.gov
Valerie	Beck	vjb@cpuc.ca.gov
Wendy	Al-Mukdad	wmp@cpuc.ca.gov
BRYAN	LEE	BLee@energy.state.ca.us
Allen	Benitez	ab2@cpuc.ca.gov

