STATE OF CALIFORNIA EDMUND G. BROWN JR., *Governor*

PUBLIC UTILITIES COMMISSION
505 VAN NESS AVENUE
SAN FRANCISCO, CA 94102-3298

FILED
05-06-11
02:41 PM

May 6, 2011

Agenda ID #10387
Quasi-legislative

TO PARTIES OF RECORD IN RULEMAKING 08-12-009

This is the proposed decision of President Peevey. It will not appear on the Commission's agenda sooner than 30 days from the date it is mailed. The Commission may act then, or it may postpone action until later.

When the Commission acts on the proposed decision, it may adopt all or part of it as written, amend or modify it, or set it aside and prepare its own decision. Only when the Commission acts does the decision become binding on the parties.

Parties to the proceeding may file comments on the proposed decision as provided in Article 14 of the Commission's Rules of Practice and Procedure (Rules), accessible on the Commission's website at www.cpuc.ca.gov. Pursuant to Rule 14.3, opening comments shall not exceed 25 pages.

Comments must be filed pursuant to Rule 1.13 either electronically or in hard copy. Comments should be served on parties to this proceeding in accordance with Rules 1.9 and 1.10. Electronic and hard copies of comments should be sent to ALJ Sullivan at tjs@cpuc.ca.gov and President Peevey's advisor Carol Brown at cab@cpuc.ca.gov. The current service list for this proceeding is available on the Commission's website at www.cpuc.ca.gov.

/s/ CHARLOTTE TERKEURST for KVC
Karen V. Clopton, Chief
Administrative Law Judge

KVC:tcg

Attachment

Decision **PROPOSED DECISION OF PRESIDENT PEEVEY** (Mailed 5/6/2011)

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)

DECISION ADOPTING RULES TO PROTECT THE PRIVACY AND SECURITY OF THE ELECTRICITY USAGE DATA OF THE CUSTOMERS OF PACIFIC GAS AND ELECTRIC COMPANY, SOUTHERN CALIFORNIA EDISON COMPANY, AND SAN DIEGO GAS & ELECTRIC COMPANY

TABLE OF CONTENTS

Title **Page**

TABLE OF CONTENTS

Title **Page**

TABLE OF CONTENTS

Title **Page**

DECISION ADOPTING RULES TO PROTECT THE PRIVACY AND SECURITY OF THE ELECTRICITY USAGE DATA OF THE CUSTOMERS OF PACIFIC GAS AND ELECTRIC COMPANY, SOUTHERN CALIFORNIA EDISON COMPANY, AND SAN DIEGO GAS & ELECTRIC COMPANY

1. Summary

This decision adopts rules to protect the privacy and security of customer usage data generated by Smart Meters deployed by Pacific Gas and Electric Company (PG&E), Southern California Edison Company (SCE), and San Diego Gas & Electric Company (SDG&E). The rules adopted implement the protections ordered by Senate Bill 1476 (Chapter 497, Statutes of 2010) and are also consistent with other sections of the Public Utilities Code and past Commission privacy policies. Attachment D lists the adopted privacy and security rules.

The adopted privacy and security rules apply to PG&E, SCE, and SDG&E, the companies that assist them in utility operations, companies under contract with the utilities, and other companies that, after authorization by a customer, gain access to the customer's usage data from the utility either via the internet or though a connection with the Smart Meter that forwards that data without further customer action (such as through a device "locked"[1] to a service provider). Each utility must file an advice letter within 90 days to bring its policies, practices and applicable tariffs into conformity with the privacy and security rules adopted here.

In addition to the adopted rules protecting the privacy and security of usage data, the decision adopts policies to govern access to customer usage data by customers and by authorized third parties. PG&E and SCE must continue to

[1] A device is "locked" to a service provider if that particular device can only be used by that single provider of energy services. This definition follows that used in wireless telecommunications, in which a "locked" wireless phone will only work on one company's network.

provide and SDG&E must provide access to customer usage data. Each utility must provide pricing, usage and cost data to customers in the customer-friendly manners discussed below. Specifically, PG&E, SCE, and SDG&E must offer residential customers bill-to-date, bill forecast data, projected month-end tiered rate, a rate calculator, and notifications to customers as they cross rate tiers. They are directed to work with the California Independent System Operator to improve customer access to wholesale electricity prices. PG&E, SCE, and SDG&E each must file an advice letter within six months that provides customers with access to usage, price, and billing data. Each must also commence a pilot study within six months on how to provide real-time or near real-time pricing information to customers.

The decision also adopts a framework to allow customers to authorize third parties who agree to comply with the adopted privacy and security rules to receive usage data from utilities via the "backhaul."[2] SDG&E must continue to provide third parties access to customer usage data and PG&E and SCE must initiate such a service. PG&E, SCE, and SDG&E must each file an advice letter within six months that creates a tariff to provide third parties, with customer authorization, with usage and billing information consistent with the polices and rules adopted to protect the privacy of customers. The decision orders the three utilities to commence pilot studies within six months to connect Home Area Network-enabled devices to Smart Meters.

The decision also adopts reporting and audit requirements regarding the utilities' customer data privacy and security practices, third-party access to

[2] A third party receives data via the "backhaul" when, after the utility hauls that data back from its Smart Meter to the utility's server, the utility then processes the data and provides it to the third party.

customer usage information, and any security breaches of customer usage information.

The adopted privacy and security rules and policies providing access to billing and usage data are reasonable. They will protect the privacy and security of customer usage data while ensuring customer access and enabling utilities and authorized third parties to use the information to provide useful energy management and conservation services. In addition, the rules and policies are consistent with privacy and security principles adopted by the Department of Homeland Security and with the policies adopted in Senate Bill 1476. Thus, these rules will bring California practices into conformity with the best national privacy and security practices.

Finally, this decision does not adopt rules and policies that apply to other electrical corporations in addition to PG&E, SCE, and SDG&E, and to gas corporations, community choice aggregators, and electric service providers. This decision, however, commences a new phase of this proceeding to explore whether the rules and policies adopted in this decision should apply to these entities.

2. Background: The Evolution of the Question of How to Promote Private, Secure, Useful and Timely Access to Electricity Usage Data

The changing laws and policies pertaining to the Smart Grid have complicated the procedural history of this proceeding and have altered the shape of the issues that the Commission must address. This section describes the procedural and statutory history that is relevant for developing Smart Grid policies to protect the privacy and security of usage data and to permit customers and authorized third parties to access that usage data.

With the enactment of Senate Bill (SB) 1476 (Padilla),[3] compliance with its specific requirements became a major aspect of the Commission's efforts to ensure that the privacy and security rules adopted by the Commission protect consumers.

The origins of the privacy and security issues in this proceeding, however, preceded the enactment of SB 1476.[4] On July 30, 2010, an Assigned Commissioner and Administrative Law Judge's Joint Ruling (Joint Ruling) set a Prehearing Conference (PHC) for August 20, 2010 to consider issues relating to data privacy, security of the Smart Grid, and access to data by customers and third parties. The Joint Ruling also invited the filing of PHC Statements no later than August 13, 2010. Thus, the Joint Ruling set as a central issue in this phase of the proceeding the determination of the best ways to implement and use Smart Grid technologies to promote California's energy policies while protecting consumer interests.

In advance of the PHC, CTIA – The Wireless Association; AT&T California (U1001C), AT&T Communications of California, Inc. (U5002C), and New Cingular Wireless PCS, LLC (U3060C) (filing jointly as AT&T); the Consumer Federation of California (CFC); Pacific Gas and Electric Company (U39E) (PG&E); Southern California Edison Company (U338E) (SCE); the Technology Network (TechNet); Tendril Networks Inc. (Tendril); San Diego Gas & Electric Company (U902E) (SDG&E) and Southern California Gas Company (U904G) (SoCalGas), filing jointly; The Utility Reform Network (TURN); the Division of Ratepayer Advocates (DRA); the Center for Democracy & Technology and the Electronic Frontier Foundation, filing jointly (CDT/EFF); the California

[3] Chapter 497, Statutes of 2010.

[4] SB 1476 was signed by the Governor and chaptered on September 29, 2010.

Independent System Operator (CAISO); and OPOWER, Inc. (OPOWER) provided PHC Statements.

On August 20, 2010, a PHC took place in San Francisco. At the PHC, parties constructively discussed the steps needed to establish a record to permit the Commission to decide issues associated with customer and third-party access to usage data and the related issues of privacy and security. The most constructive suggestions to emerge in the PHC were those that recommended that the Commission stop further consideration of abstract principles and instead focus on issues related to privacy and security protections for the usage data generated by Smart Meters and communicated on the Smart Grid. These suggestions called for a direct consideration of the proposed uses of the Smart Grid data and the planned access to the data that a utility will provide to customers and to third parties.[5]

On September 27, 2010, an Assigned Commissioner's Ruling (ACR) ruled that PG&E, SCE, and SDG&E must file comments on certain privacy and access questions. In addition, the ACR ordered PG&E to provide an overview of the statutory scheme adopted in California to protect customer privacy. The ACR also ordered SDG&E to provide information on its program that offers third-party access to usage data. The ACR also invited proposals from any party that would help ensure the security of customer data while permitting access to the information by authorized third parties. These comments were due on October 15, 2010.

[5] The focus on the specific usage data generated by the Smart Meters and its concrete uses is the analytic approach adopted in this decision. At every point, the decision seeks to avoid discussion of abstractions and instead focuses on actions needed to protect usage and personal data.

On September 29, 2010, SB 1476[6] was signed into law and chaptered by the Secretary of State. SB 1476 added sections 8380 and 8381 to the Pub. Util. Code. These new sections addressed issues of privacy arising from the use of Smart Meters.

On October 15, 2010, the Local Government Sustainability Energy Coalition, OPOWER, PG&E, Utility Consumer Action Network (UCAN), Verizon California Inc. (Verizon),[7] TechNet, Tendril, SCE, CDT/EFF, CFC, DRA, SDG&E, EnerNOC, Inc. (EnerNOC), AT&T, TURN, California Large Energy Consumers Association (CLECA) filed opening comments.[8] In addition to the information sought by the ACR, PG&E's review of applicable statutes provided many details concerning the newly enacted SB 1476 and other statutes that create a framework to protect consumer privacy.

On October 25 and 26, 2010, workshops took place in which parties discussed the proposals contained in the opening comments and the requirements of SB 1476.

Because of regulatory and legal complexities that the workshops identified, an ALJ Ruling on October 29, 2010 extended the deadline for reply comments to November 8, 2010 and established a briefing cycle for parties to address issues concerning the extent of the Commission's authority over entities

---

[6] SB 1476 is appended to this decision as Attachment A.

[7] Verizon consists of a group of licensed utilities in California consisting of California RSA No. 4 Limited Partnership, Cellco Partnership, Fresno MSA Limited Partnership, GTE Mobilnet of California Limited Partnership, GTE Mobilnet of Santa Barbara Limited Partnership, Los Angeles SMSA Limited Partnership, MCI Communications Services Inc., Modoc RSA Limited Partnership, Sacramento Valley Limited Partnership, Verizon California Inc., Verizon Wireless (VAW) LLC and WWC License L.L.C.

[8] All references to Opening Comments in this document will refer to the responses filed on October 15, 2010, unless otherwise noted.

that acquire access to information on a consumer's energy usage either through the utility or through some other means.

By November 8, 2010, the Center for Energy Efficiency and Renewable Technologies (CEERT), TURN, AT&T, the Future of Privacy Forum, CDT, SCE, PG&E, the State Privacy & Security Coalition and TechNet (filing jointly), Verizon, CAISO, CFC, EnerNOC, UCAN, SoCalGas, DRA, Control4 Corporation (Control4), and SDG&E filed reply comments.[9]

By November 22, 2010, responding parties filed opening briefs on jurisdictional issues. Several parties filed jointly together. Specifically, the high technology parties EnerNOC, TechNet, Control4 and Tendril (Technology Companies) filed jointly. The consumer groups DRA, TURN and UCAN (Customer Representatives) also filed jointly. Verizon and AT&T (Telephone Companies) also filed jointly. SDG&E and SoCalGas (Sempra Utilities) also filed jointly. PG&E, SCE, and CFC filed separate briefs.

By December 6, 2010, parties filed reply briefs. The Technology Companies filed a joint reply brief. The Customer Representatives also filed a joint reply brief. The Telephone Companies filed a joint reply brief. The Future of Privacy Forum, SCE, and CFC separately filed reply briefs.

On January 1, 2011, SB 1476 went into effect.

3. Commission's Authority over Smart Grid Issues Enhanced and Clarified by Recent Legislation

As noted above, recent legislation including SB 1476, SB 17 (Padilla)[10] and the Energy Independence and Security Act of 2007[11] have addressed issues

[9] Throughout this document, unless otherwise noted, Reply Comments will refer to the reply comments filed on November 8, 2010.

[10] Chapter 327, Statutes of 2009.

arising from the Smart Grid and have required both interpretation and implementation throughout this proceeding. In addition, the Pub. Util. Code and past Commission decisions reflect California's long-standing interest in the protection of the privacy of utility customers.

Because of the recency of some statutory provisions and the long-standing nature of other privacy and security policies, it is prudent to review the relationship between the Fair Information Practice (FIP) Principles, endorsed in Decision (D.) 10-06-047, and applicable statutes and past Commission decisions that apply to the privacy issues posed by Smart Meters and the Smart Grid. Such a review can help ensure a regulatory approach consistent with law and precedent, determine whether the FIP principles are consistent with SB 1476, and determine whether the FIP principles can be used to develop privacy rules consistent with statutory requirements.

3.1. SB 1476 Seeks to Protect the Privacy of Usage Information

SB 1476 contains a preface that explains the legislative intent of § 8380, a section that it adds to the Pub. Util. Code:

> This bill would prohibit an electrical corporation or gas corporation from sharing, disclosing, or otherwise making accessible to any 3rd party a customer's electrical or gas consumption data, as defined, except as specified, and would require those utilities to use reasonable security procedures and practices to protect a customer's unencrypted electrical and gas consumption data from unauthorized access, destruction, use, modification, or disclosure.
>
> The bill would prohibit an electrical corporation or gas corporation from selling a customer's electrical or gas consumption data or any other personally identifiable information for any purpose.

---

[11] 16 U.S.C. § 2621(d).

> The bill would prohibit an electrical corporation or gas corporation from providing an incentive or discount to a customer for accessing the customer's electrical or gas consumption data without the prior consent of the customers.
>
> The bill would require that an electrical or gas corporation that utilizes an advanced metering infrastructure that allows a customer to access the customer's electrical and gas consumption data to ensure that the customer has an option to access that data without being required to agree to the sharing of his or her personally identifiable information with a 3rd party.
>
> The bill would provide that, if the electrical corporation or gas corporation contracts with a 3rd party for a service that allows a customer to monitor his or her electricity or gas usage, and the 3rd party uses the data for a secondary commercial purpose, the contract between the electrical or gas corporation and the 3rd party shall provide that the 3rd party prominently discloses that secondary commercial purpose to the customer.[12]

This clear statement of policy guides our implementation of § 8380.

3.2. Are FIP Principles Consistent with SB 1476 and Other California Statutes?

On March 9, 2010, CDT/EFF filed comments in this proceeding proposing that the Commission adopt FIP principles to protect the privacy of consumers. CDT/EFF noted that these FIP principles were adopted by the Department of Homeland Security and argued that "a framework developed for information systems affecting the national security is also well-suited to the issues posed by the Smart Grid."[13]

CDT/EFF stated that "[t]he DHS framework includes the following eight principles: (1) Transparency, (2) Individual Participation, (3) Purpose

[12] SB 1476, Chapter 497 of Statutes of 2010, pages 1-2.

[13] Joint Comments of the Center for Democracy & Technology and the Electronic Frontier Foundation on Proposed Policies and Finding Pertaining to the Smart Grid, March 9, 2010, at 15.

Specification, (4) Data Minimization, (5) Use Limitation, (6) Data Quality and Integrity, (7) Security, and (8) Accountability and Auditing."[14]

In October 15, 2010 Comments, the CDT/EFF renewed its request that the Commission adopt the FIP principles and demonstrated how these principles could lead to specific proposals to protect privacy.[15]

PG&E, at the request of the ALJ, provided a compendium of California law and Commission decisions applicable to privacy practices pertaining to the usage of electricity consumers as part of its opening response to the September 27, 2010 ACR.[16] Subsequently, in preparation for the October 25-26 workshops, PG&E mapped California statutes to the FIP principles,[17] as follows:

1. **Transparency –** SB 1476, Pub. Util. Code § 8380(c) adopts requirements that make the use of a consumer's energy data transparent to the consumer. Section 8380(c) states: "If an electrical corporation or gas corporation contracts with a third party for a service that allows a customer to monitor his or her electricity usage, and that third party uses the data for a secondary commercial purpose, the contract between the

---

[14] *Id*.

[15] Proposed Smart Grid Privacy Policies and Procedures: Opening Response of the Center for Democracy & Technology and the Electronic Frontier Foundation to Assigned Commissioner's Ruling of September 27, 2010, at Appendix A, pages 1-4.

[16] Opening Responses of Pacific Gas and Electric Company to Assigned Commissioner's Ruling on Customer Privacy and Security Issues, October 15, 2010, Appendix A: List of Current Statutes, Regulations, Decisions and Protocols Related to Customer Privacy Applicable to California Energy Utilities. We have included this as Attachment B to this decision.

[17] This information was contained in a power point presentation made by PG&E at the workshop. The presentation was titled "Consumer Privacy Policy" and was made available to all parties through posting on the Commission's website. As of February 3, 2011, the presentation was available at http://www.cpuc.ca.gov/NR/rdonlyres/9B3563D4-5C59-4FD7-8DC4-24422AB6EFE2/0/PrivacyWorkshop_Oct2520103.pdf.

electrical corporation or gas corporation and the third party shall provide that the third party prominently discloses that secondary commercial purpose to the customer."

CA Business and Professions Code § 22575 requires online posting of a privacy and third-party access policies of California businesses, including energy utilities.

2. **Individual Participation** – SB 1476 , Pub. Util. Code § 8380(b)(1) anticipates the participation of individuals in protecting their own privacy by requiring a customer's consent before disclosure of information to a third party. Section 8380(b)(1) states: "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."

   CA Civil Code Section 1633.1 et seq. – authorizes the use of electronic transactions/signatures to satisfy laws requiring records to be in writing.

3. **Purpose Specification** – SB 1476, Pub. Util. Code § 8380(e)(2) designates certain purposes for which disclosure of usage information is expected and automatically approved. Section 8380(e)(2) states: "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."

4. **Data Minimization** – Although a principle of data minimization is not explicitly required in SB 1476, Commission actions frequently set requirements concerning the collection, retention

and reporting of data. Commission rate cases, general regulation, and the Pub. Util. Code often state periods for data retention or reporting of data. For example, Pub. Util. Code § 6354(e), which states: "Energy utilities must report to municipalities the names and addresses of customers who transport gas or electricity, for the purposes of enforcing taxes and fees. Municipalities shall not disclose such customer information to third parties." Thus, even if policies of data minimization are not explicitly contained in SB 1476, data collection and retention, the key to a FIP of data minimization, certainly falls within the purview of the Commission.

5. **Use Limitation –** SB 1476, Pub. Util. Code § 8380(e) (2) – cited above, limits the use of electricity usage information. Specifically, § 8380(e) (2) prohibits the use of energy consumption data for a secondary commercial purpose not related to the primary purpose of the contract without the customer's consent.
6. **Data Quality and Integrity –** Although a principle supporting data quality and integrity is not explicitly required in SB 1476, Commission regulation of utility operations and services requires the accuracy of underlying information. Most directly, it is clear that ensuring the accuracy of data is consistent with consumer protection initiatives in the Pub. Util. Code that require that rates and bills be reasonable.
7. **Data Security –** SB 1476, Pub. Util. Code § 8380(d) explicitly calls for keeping the information associated with the smart grid safe. Section 8380(d) states: "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."

In summary, the FIP principles are closely related to SB 1476 and the consumer protection initiatives that have developed out of the Pub. Util. Code, and each principle is supported by law and precedent.

3.3. Should the Commission Use FIP Principles to Develop Privacy and Security Regulations?

With the passage of SB 1476, an issue arose in this proceeding over whether to adopt the FIP principles and then develop regulations proceeding from the principles, or whether to proceed directly from the statute to the regulations.

CDT/EFF was the first to address this matter, and presented proposed rules in their Opening Comments. A goal of CDT/EFF's comments and proposed rules was to operationalize the FIP principles. In Reply Comments, CDT further argued that the rules proposed by CDT/EFF constitute "a concrete set of Smart Grid privacy safeguards, based on the widely accepted Fair Information Practice principles."[18]

CDT's presentation of its rules relied on the FIP principles, thereby demonstrating the usefulness of these principles for developing rules to protect the privacy and security of energy usage information.

DRA argued that the Commission has already decided the issue of whether to rely on the FIP principles. DRA claimed that D.10-06-047 adopted the FIP principles "as a framework for privacy rules"[19] and recommended that the Commission simply proceed "to adopt more specific rules."[20]

Other consumer groups also supported the FIP principles. UCAN strongly supported the FIP principles in Opening Comments, stating:

[18] CDT Reply Comments at 1.

[19] DRA Reply Comments at 1.

[20] *Id.*

> For the purposes of protecting personal information, a time-tested approach to policy development is to utilize the Principles of Fair Information Practices.[21]

TURN similarly supported the CDT/EFF proposed rules based on the FIP principles, stating:

> TURN has reviewed a draft of the comments being submitted by the CDT/EFF and strongly supports their proposed rules that operationalize the Fair Information Practice Policies.[22]

The Future of Privacy Forum also endorsed the FIP principles, stating:

> We encourage the Commission to adopt rules that encompass the principles embodied in the well-accepted Fair Information Practice Principles, covering all collection, use, retention, and sharing of data.[23]

In the wake of the adoption of SB 1476, PG&E provided a workshop presentation, summarized above, to show how SB 1476 provides statutory support for the major elements of the FIP principles. Subsequently, PG&E argued that it "jointly presented [with CDT] a draft of privacy principles which reflected …a possible consensus for adoption by the Commission."[24]

SCE also responded favorably to the usage of the FIP principles. SCE stated that SCE "focuses its reply on customer data privacy issues on CDT's 'straw' proposal,"[25] which was built on the FIP principles. Thus, SCE's proposals implicitly presume that the FIP principles are reasonable guiding principles for privacy and security rules.

---

[21] UCAN Opening Comments at 5.

[22] TURN Opening Comments at 5.

[23] Future of Privacy Forum Reply Comments at 2.

[24] PG&E Reply Comments at 1.

[25] SCE Reply Comments at 2.

Not all parties, however, took such a supportive approach to the FIP principles. SDG&E, in particular, urged a more tentative approach to the adoption of the FIP principles. SDG&E argued:

> SDG&E agrees in principle with the efforts made by CDT & EFF in their proposal, but suggests that the scheme requires further analysis in order to achieve greater consistency in provisions and reasonably accommodation before the [Commission] considers establishing electric utility operational FIPs.[26]

SDG&E, a member of Sempra Utilities, urged caution, stating:

> At a minimum, SDG&E submits that a technical working group should be established to create a common "straw man proposal" or set of "use cases" to foster a better overall understanding of how the FIP's privacy principles may be implemented or applied to the electric IOUs.[27]

SoCalGas, another member of the Sempra Utilities, expressed skepticism concerning the ability of the Commission to make operational the FIP principles. SoCalGas argued:

> SoCalGas believes that current laws are sufficient and adequate enough to protect the customer's privacy. Overall, SoCalGas agrees with the Center for Democracy and Technology and Electronic Frontier Foundation proposal and the Fair Information Practice principles, however, the intentional vagueness of the proposal, although accommodating a myriad of circumstances, is not specific enough for implementation. SB 1476 is sufficient for the operation of the gas [Advanced Meter Infrastructure] network to be deployed by SoCalGas pursuant to D.10-04-027.[28]

---

[26] SDG&E Reply Comments at 5

[27] *Id*. The terms "investor owned utility" (IOU) and "utility" are used interchangeably in this decision.

[28] SoCalGas Reply Comments at 3.

More specifically, SoCalGas stated that:

> SoCal Gas does not believe that the Commission has yet provided a clear direction that the policies being considered in this proceeding should be expanded beyond the electric grid system. Conversely if the Commission wants to apply the FIP's standards to gas corporations, then SoCalGas would urge those issues be further discussed, analyzed or vetted within the gas service provider context.[29]

EnerNOC also saw no need for addressing FIP principles, and instead argued:

> The Commission should focus on implementing SB 1476 as simply and as quickly as possible. No further restrictions or privacy protections are needed, especially in the CI&I sector.[30]

CEERT advocated a more mixed position. CEERT did not object to the FIP principles, and argued that: "Fair Information Principles practices are a good basis for protecting customer privacy, if necessary, but NIST [National Institute of Standards and Technology] cyber-security standards should form the basis of keeping customer data secure."[31] On the other hand, CEERT also argued that "… SB 1476, therefore, does not signify that this Commission is authorized to identify all 'potential' abuses related to 'energy consumption data,' but rather is required to follow the express dictates of Section 8380 in terms of adopting rules applicable to jurisdictional IOUs."[32]

AT&T did not directly address the FIP principles and their relationship to SB 1476. Instead, AT&T summarized its position on privacy and security as:

---

[29] *Id*. at 5.

[30] EnerNOC Reply Comments at 8.

[31] CEERT Reply Comments at 2.

[32] *Id*. at 6.

> AT&T encourages the Commission to avoid the adoption of rigid, burdensome consumer privacy rules. Instead, the Commission should seek to adopt a simple framework based on the requirements of SB 1476.[33]

Verizon, similarly, did not object to FIP principles, but cautioned that "overly broad and granular rules … will stifle the development of innovative new products and services without providing useful benefits to consumers."[34]

3.4. Discussion: FIP Principles are Consistent with Pub. Util. Code and Offer a Good Basis for Developing Privacy and Security Regulations

This decision adopts the FIP principles as guides for developing California policies and regulations that aim to protect the privacy and security of the electricity usage data of consumers.

The analysis conducted by PG&E and other parties in this proceeding allows us to affirm that the FIP principles are consistent with SB 1476, the Pub. Util. Code, and emerging national privacy and security practices.

Moreover, the comments and discussion of the parties permit us to remove any uncertainty concerning the utility of the FIP principles for development of a regulatory program to protect privacy. D.10-06-047 took the first step towards adopting the FIP principles as the framework for privacy policy in California. D.10-06-047 states:

> … we agree with CDT-EFF and Researchers that an assessment of privacy and grid security issues should be included as part of this baseline report.[35]

---

[33] AT&T Reply Comments at 2.

[34] Verizon Reply Comments at 9.

[35] D.10-06-047 at 41.

D.10-06-047 then noted, with favor, that:

> CDT-EFF suggests that this privacy assessment should be responsive to the principles outlined in the Fair Information Practices.[36]

D.10-06-047, however, did not clearly adopt the FIP principles as California policy for the Smart Grid. This decision does so now.

PG&E's analysis, quoted above, links five of the seven FIP principles to specific statutory provisions in SB 1467 and the Pub. Util. Code. This analysis makes it clear that these five principles – Transparency, Individual Participation, Purpose Specification, Use Limitation and Data Security – are consistent with California statutory requirements and are necessary for ensuring that a regulatory program to promote policy meets the statutory requirements of the Pub. Util. Code.

The two principles not specifically linked to statutory requirements in the analysis above – Data Minimization and Data Quality and Integrity – are also reasonable principles and consistent with California law and policy objectives. A principle and practice of "Data Minimization" will clearly promote the security of data. Limiting the collection of personal data to just what is needed reduces the amount of data that requires protection and reduces the risks that arise from a security breach. Thus, a principle of data minimization follows directly from the public interest in keeping data secure.

The FIP principle of promoting Data Quality and Integrity is also both reasonable and consistent with California law. Data quality and integrity are critical to the rendering of accurate and reasonable bills. Moreover, accurate data

[36] *Id*.

helps protect consumers from the adverse consequence of false consumption and payment data.

In conclusion, this decision adopts the FIP principles as the key framework for developing specific regulations to protect consumer privacy because these principles are consistent with California law, consistent with emerging national privacy and security policies, and supported by the record in this proceeding. A statement of the FIP principles brings clarity to the goals of California privacy and security regulations. A subsequent section of this decision will adopt regulations to protect privacy and security that operationalize the FIP principles. Our ability to translate the principles into a regulatory program belies the criticisms that the FIP principles are "not specific enough for implementation." [37]

4. Jurisdiction: What is the Extent of the Commission's Authority and Obligation to Protect Confidential Consumer Information?

The technology of the Smart Grid and the participants in Smart Grid include companies other than investor owned utilities. In addition, much state and federal legislation is new to this area. In light of the novelty of this technology and the laws setting policy, it is unsurprising that legal issues arise over the extent of the Commission's jurisdictional authority over data generated by Smart Meters. As noted in the procedural history section above, the Commission asked parties to brief issues pertaining to the Commission's jurisdiction over the data created by Smart Meters and over those obtaining access to this data, either through the utilities or through some other means. A goal of this briefing cycle was to clarify jurisdictional issues arising from new

[37] SoCalGas Reply Comments at 3.

laws and new technologies in order to ensure that the Commission possesses the statutory authority necessary to support the program that it adopts.

The record in this proceeding has demonstrated that the data on energy consumption generated by Smart Meters and transmitted by the Smart Grid will prove critical to future conservation and grid management efforts. Enabling consumers and companies to assess and act on this information is key to advancing many of California's energy policies, such as promoting conservation, reducing demand in response to grid events and price signals, reducing summer peak demands, and efficiently incorporating renewable energy and electric vehicles into grid operations.

Our investigation shows that access to detailed, disaggregated data on energy consumption can reveal some information that people may consider private. Thus, the inadvertent release or the theft of this data could provide information that diminishes the privacy of electricity users.

The workshops on privacy in this proceeding held on October 25 and 26, 2010, uncovered substantive disagreements over the reach of the Commission's authority and the Commission's ability to protect the privacy of the information that is generated by the Smart Meters and transmitted through the Smart Grid. Subsequent to the workshops, an October 29, 2010 ALJ Ruling posed two questions for the parties to this proceeding to brief:

1) What authority does the Commission have over entities that receive information on a consumer's energy usage from the utility? What actions, if any, can the Commission take in response to misuse of data by such an entity?
2) What authority, if any, does the Commission have over entities that receive information on a consumer's energy usage from sources other than the utility (from a HAN device or from the customer, for example)? What actions, if any, can the

> Commission take in response to misuse of data by such an entity?[38]

Opening Briefs were due by November 22, 2010 and Reply Briefs were due by December 6, 2010.

4.1. Arguments of Parties in Briefs

The briefs filed in this proceeding included a mix of statutory and policy analysis. As they did in the workshops, parties differed substantially in their views concerning the authority of the Commission to protect the data generated by Smart Meters and the prudency of adopting far-reaching rules at this time.

There was, however, little controversy concerning the authority of the Commission to protect the privacy of information in the hands of the utility. The argument in support of Commission authority over usage data in the hands of the utility was perhaps most forcefully made by the Customer Representatives. The Customer Representatives argued that the discussion at the workshops "made clear that if the IOU or its contractor receives data generated from smart meters or related devices, the Commission has full jurisdiction to apply and enforce privacy rules."[39] To a large extent, this is the practice in place for data generated today in the course of the utility's business.

The Customer Representatives argued further that "[t]he real issue for decision is whether the Commission can apply and enforce rules on parties who seek energy usage data directly from the customer, and who are not in privity/contract with the IOUs."[40] The Customer Representatives argued that

---

[38] ALJ Ruling, October 29, 2010, at 2.

[39] Customer Representatives Opening Brief at 3.

[40] *Id*. at 5.

the Commission has the authority "to adopt privacy rules applicable to all parties that seek to possess and use Smart Grid-related data."[41]

This position was opposed by many parties, and the central issue that was disputed in briefs was what authority the Commission has over those entities not involved in utility operations that have obtained customer approval to access their usage data.

On this matter, the Customer Representatives argued that the Commission has authority over those who have access to usage data. The Customer Representatives articulated a three step argument in their Opening Brief that supports their expansive interpretation of the statutory authority of the Commission, arguing that the authority of the Commission reaches anyone with the data. The argument goes as follows:

> Step 1: Pub. Util. Code Section 701 confers broad power on the Commission to regulate public utilities.[42]
>
> Step 2: "In *PG&E Corp v. Public Utilities Comm.,*[43] the court made clear that the Commission may enforce conditions against non-public utilities (in that particular case, utility holding companies) where such jurisdiction was not barred by statute and was essential to the Commission's assertion of regulatory authority over utilities. 118 Cal. App. 4th at 1199."[44] This court decision established the "cognate and germane" criteria (discussed below) for determining the reach of Commission authority.
>
> Step 3: The regulation of third parties interaction with customers over access to their energy usage data "is an exercise of authority that is cognate and germane to the Commission's regulation of IOUs [investor owned utilities] and therefore permissible under Public

---

[41] *Id*. at 3.

[42] *Id*. at 5.

[43] *PG&E Corp. v. Public Utilities Com.* (2004) 118 Cal. App. 4th at 1174.

[44] Customer Representatives Opening Brief at 5..

> Utilities Code § 701."[45] Therefore, the Commission has authority over any third party who obtains access to a customer's energy usage data.

In addition to this legal argument based on § 701 and court precedent, the Customer Representatives argued that SB 1476 strengthens the Commission's jurisdiction over third parties because it "reaffirmed the importance of protecting customer's privacy rights inherent in Smart Grid data." The Customer Representatives contended that although the statute is silent on the full extent of authority over third parties, the legislative history states that the bill:

> would provide that a customer's electric or gas consumption data shall be securely kept by the local publicly owned electric utility or electrical or gas corporation and shall not be accessible by a third party, unless a customer chooses to access his or her consumption data from a third party using a smart meter, after being given the option not to relinquish his or her data.[46]

The Customer Representatives contended that this legislative intent, combined with the statutory authority conveyed, has provided the Commission with full authority to protect consumers by regulating access to and the use of electricity consumption data by any party in its possession.

Finally, the Customer Representatives argued that the Commission has a "long-standing enforcement obligation to protect California's electric customers."[47] To meet this obligation, Customer Representatives recommended that the Commission "[a]dopt a registration process for all third parties seeking

---

[45] *Id*. at 8.

[46] *Id*. at 11, quoting from Excerpts from Bill Analysis of Senate Judiciary Committee, SB 1476 (Padilla), 2009-2010 Regular Session, available at http://www.leginfo.ca.gov/pub/09-10/bill/sen/sb_1451-1500/sb_1476_cfa_20100412_120118_sen_comm.html .

[47] *Id*. at 12.

customer Smart Grid data and ensure that oversight agencies will enforce customers' privacy rights against any third-party party [sic] that misuses their energy consumption or other energy-related data."[48]

CFC, like the Customer Representatives, argued that there is broad Commission authority over any third party who acquires data on energy consumption, no matter what the source. CFC also argues that regulation to protect the privacy of this data is "cognate and germane" to the exercise of the Commission's regulatory authority.[49]

SCE's Opening Brief offered a detailed analysis of the jurisdictional questions posed in the ACR. In response to Question 1 – Commission authority over those obtaining consumption data from the utility – SCE argued that Commission authority over utilities and their contractors is well settled. Concerning Commission authority over other third parties, SCE argued that "absent a statutory grant of authority, the Commission has no jurisdiction to enforce the consumer protections compliance of these third parties."[50] SCE, however, noted that this is not the end of the story because "the Commission has full authority to establish IOU tariffs governing third-party access to customer data from the IOUs"[51] and that "tariffs can authorize the IOUs – and advise or require customers – to take appropriate precautions in releasing customer data to third parties.[52]

---

[48] *Id*. at 15.

[49] CFC Opening Brief at 7.

[50] SCE Opening Brief at 2.

[51] *Id*.

[52] *Id*.

In response to question 2 – concerning Commission authority over entities that acquire consumption data through channels that do not include the utility – SCE argued that "absent a statutory grant of authority, the Commission has no jurisdiction to enforce the consumer protections compliance of these third parties."[53] Here, however, SCE found that "the Commission has full authority to direct the IOUs to help customers"[54] because "[c]ustomer awareness is likely to be one of the most effective tools against misuses of customer data by third parties."[55]

PG&E's Brief, rather than arguing for a single position concerning Commission jurisdiction, presented arguments for and against the Commission's authority to enforce privacy rules in specific situations and identified approaches that permit the Commission, in its view, to exercise authority over the terms of data use without incurring a high litigation risk.

PG&E found that the nexus between the utility and its provision of consumption data to a third party can extend Commission jurisdiction to the third party. PG&E argued that based on its reading of *Hillsboro*[56] and *PG&E Corp.*,[57] "the regulation of the third party's use and access to the information is arguably 'cognate and germane' to the jurisdictional activities of the utility itself."[58] PG&E, however, also argued that:

> …the recent enactment of Public Utilities Code Section 8380 by the California Legislature calls into question whether that reach extends

---

[53] *Id*.

[54] *Id*.

[55] *Id*.

[56] *Hillsboro Properties v. Public Utilities Com*. (2003) 108 Cal. App. 4th at 246.

[57] *PG&E Corp. v. Public Utilities Com.* (2004) 118 Cal. App. 4th at 1174.

[58] PG&E Opening Brief at 3.

> to non-utilities even when they receive consumer energy usage information directly from a utility. Under the canon of statutory construction *expressio unius est exclusio alterius*, the fact that Section 8380 confers authority on the Commission to directly regulate utilities but not their non-utility agents and contractors, arguably would support a conclusion that the Legislature intends the Commission to only regulate utilities on these matters.[59]

Like SCE, PG&E found a resolution to this potentially limited authority in tariffs:

> … for nearly twenty years, [Commission]-jurisdictional utilities have implemented specific tariffs and other restrictions on access to customer-specific information under Commission rules and orders. To the extent these tariffs and underlying Commission rules and orders dictate the terms and conditions of non-utility access to consumer energy usage information, any breach of those access restrictions can be remedied by a Commission order enjoining a utility from continuing to provide such information to the non-utility. [60]

Thus, PG&E ultimately found merit to the argument that the Commission's authority over tariffs can be used to promote the privacy of consumer data.

PG&E argued that the Commission's authority over third parties that acquire consumption information from a customer device is limited, arguing that "… the Commission's interest and jurisdiction to regulate that appears more attenuated than other utility-related regulations."[61] On the other hand, PG&E noted that the utility can control the access of any device to the Smart Meter, and PG&E contends that "the Commission could attempt to indirectly regulate the privacy of information generated by HAN-enabled or other commercially

[59] *Id*. at 4, footnote omitted.

[60] *Id*. at 6.

[61] *Id*. at 8.

available consumer devices 'beyond the meter' through conditions applied to a utility's registration of such devices on its Home Area Network."[62]

The Sempra Utilities also argued that the Commission has clear authority over the uses of data by the utility or by those in contract to the utility to perform a utility operation. The Sempra Utilities, however, argued that the Commission's authority over third-parties who acquire information from a non-utility measurement device, such as the commercially available "TED" device,[63] or from a customer who transfers data to a third party from a HAN that is registered with the Smart Meter, is "uncertain."[64]

The Telephone Companies argued that under SB 1476,

> … legislation prohibits utilities to "share disclose or otherwise make accessible to any third party a customer's electrical or gas consumption data" absent a contractual requirement with the third party to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information" and to "protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[65]

The Telephone Companies also argued that "new certification and reporting requirements on third parties" and prohibiting "third parties from even being allowed to seek customer consent to the use of personal data for 'secondary commercial purposes' is contrary to the plain language of SB 1476."[66] Instead, the Telephone Companies contended that "the Commission should

---

[62] *Id*. at 8.

[63] The Energy Detective (TED) device is a home energy monitor that enables the owner to see energy usage in real time. The TED device is currently commercially available.

[64] Sempra Opening Brief at 9.

[65] Telephone Companies Opening Brief at 6.

[66] *Id*. at 6.

decline to exercise that authority [§ 701] at this time in reliance on the principles of competitive and technological neutrality previously discussed."[67]

The Technology Companies also argued for a restrictive view of the Commission's authority over third-parties and their HAN networks, which they call "non-utility devices." Concerning SB 1476, the Technology Companies contended that "the Legislature has not expanded this Commission's jurisdiction to regulate customers or authorized third parties with respect to data access or their use of non-utility devices within the privacy of their homes or businesses."[68] In addition, the Technology Companies argued that "the Commission has no regulatory jurisdiction over non-utility devices or 'sources' of 'energy consumption data.'"[69]

In the Reply Briefs, parties both supported their arguments and identified the weaknesses of others and therefore this decision will not discuss each Reply Brief. One Reply Brief, however, deserves special comment. The Customer Representatives, in their Reply Brief, argued that PG&E misstated D.09-03-026 when PG&E concluded that the Commission has already endorsed the ability of third-parties to link their commercially-available HAN devices to utility Smart Meters without regulation of the customer/third party relationship. Instead, the Customer Representatives contended that D.09-03-026 "says nothing to indicate that the Commission has precluded regulation of the customer/third-party relationship."[70]

---

[67] *Id*. at 8.

[68] Technology Companies Opening Brief at 6.

[69] *Id*. at 10.

[70] Customer Representatives Reply Brief at 5.

4.2. Discussion: Jurisdiction Over Utilities and their Contractors/Agents is Clear; Tariff Provisions for Access to Data Can Limit the Registration of Third Party Controlled Home Area Networks to Entities that Respect Privacy

Because a major goal of this decision is to adopt a regulatory program to protect the privacy and security of usage data collected by the three electrical corporations that are the subject of this proceeding, the Commission need not consider the Commission's authority over data in the abstract. Instead, the Commission need only inquire as to whether the Commission has the authority to take the regulatory actions that it wants to use to protect the interests of consumers.

In the situation before us, SB 1476 provides specific guidance and grants the Commission authority to accomplish the legislative goals and requirements. The relevant sections added to the Pub. Util. Code are:

> 8380 (b)
>
> (1) An electrical corporation or gas corporation shall not share, disclose, or otherwise make accessible to any third party a customer's electrical or gas consumption data, except as provided in subdivision (e) or upon the consent of the customer.
>
> (2) An electrical corporation or gas corporation shall not sell a customer's electrical or gas consumption data or any other personally identifiable information for any purpose.
>
> (3) The electrical corporation or gas corporation or its contractors shall not provide an incentive or discount to the customer for accessing the customer's electrical or gas consumption data without the prior consent of the customer.[71]
>
> 8380 (d) An electrical corporation or gas corporation shall use reasonable security procedures and practices to protect a customer's

[71] Section 8380(b).

> unencrypted electrical or gas consumption data from unauthorized access, destruction, use, modification, or disclosure.[72]

SB 1476 also envisions that a utility may contract with third parties to conduct basic utility operations. In these situations, SB 1476 requires privacy protections similar to those under which a utility operates.

The Commission can also ensure that utility contracts, which the Commission has the authority to review, contain privacy protections:

> 8380 (e)(2) 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.[73]

If an electric utility enters into a contract with a third party to provide a service to the utility customer using the data from a Smart Meter, SB 1476 also sets specific requirements concerning what the contract must contain:

> 8380 (c) If an electrical corporation or gas corporation contracts with a third party for a service that allows a customer to monitor his or her electricity or gas usage, and that third party uses the data for a secondary commercial purpose, the contract between the electrical corporation or gas corporation and the third party shall provide that

[72] Section 8380(d).

[73] Section 8380(e)(2), emphasis added.

> the third party prominently discloses that secondary commercial purpose to the customer.[74]

This statutory language leads us to conclude that the Commission has both broad powers and a legislative mandate to develop rules and regulations to protect the usage data of utility customers vis-à-vis the utility, its operational contractors, and those with whom a utility contracts to provide energy monitoring services to utility customers.

A third party, however, can acquire consumption data from two other sources: 1) from a HAN-enabled device which obtains data from the Smart Meter and passes it on; or, 2) from the customer, who obtains it from the utility or from the Smart Meter.

A non-utility HAN-enabled device must be authorized in order to enable the direct transfer of data from the Smart Meter. The process of authorization requires that the device be "registered" by the particular smart meter. A utility will provide this registration service pursuant to utility tariffs. The Commission, as many parties have commented, has the authority to impose requirements as a tariff condition that protects the privacy and security of usage information.

This decision addresses the situation in which a customer seeks to register with the Smart Meter a HAN-enabled device that is "locked"[75] to a particular third party and automatically transfers information to that third party. The analysis below leads us to conclude that in this situation, it is reasonable that the utility tariff require as a condition for registering the device with the Smart Meter and transferring data that the third party demonstrate compliance with Commission requirements for protecting customer data and that the third party

[74] Section 8380(c).

[75] See footnote 1 for a definition of "locked."

has the consent of the consumer to the data transfer and to the proposed uses of the data.

This approach is reasonable for several reasons. First, requiring privacy protections as a tariff condition is consistent with the intent and language of SB 1476. Second, these requirements will ensure equal regulatory treatment for third parties who acquire usage data from the utility and those who acquire usage data from a device. Third, the use of tariffs to regulate the connection of devices to a network is consistent with Commission regulatory practice and well understood. Fourth, requiring that third parties who acquire usage data from a "locked" device dedicated to their energy services alone provide privacy protections to the consumer protects a consumer who invests in such a device by assuring that the third party will handle the usage data responsibly.

This decision also requires the three utilities to adopt tariff rules for HAN-enabled devices that do not automatically transfer information to a third party. If a HAN-enabled device does not have a provision for automatically transferring data to a third party, the Commission will require that the utility provide the customer (as a tariff condition and as part of the registration procedure) with information concerning the potential uses and abuses of usage data should the customer forward or otherwise provide the data to another entity. If the consumer links a HAN-enabled device to the energy services of a specific vendor, the consumer can, if the situation requires, break that link and establish a new link with a different vendor. These steps will help ensure that the customer understands and can manage the risks to privacy that this usage data can pose.

Under this approach, the Commission does not regulate what a consumer does with energy usage data. As a consequence, the Commission does not need

to determine at this time whether the Commission has the authority to regulate either the customer or other entities that acquire energy usage data from the consumer.

In summary, the Commission has authority and requires that PG&E, SCE, and SDG&E within 90 days of the mailing of this decision file advice letters to implement policies that the utility and those with whom it contracts for utility operations must follow to protect the privacy and security of consumer usage information.[76] Furthermore, the Commission has authority and requires PG&E, SCE, and SDG&E to follow rules and procedures to protect the privacy and security of consumer usage information in contracting with any third party.[77] The Commission also has authority and requires PG&E, SCE, and SDG&E to develop tariffs pertaining to the transmission of consumer usage data to third parties and tariffs for registering non-utility HAN-enabled devices that are "locked" and that automatically transfer usage information to a third party. The tariff provisions shall require that the customer agrees to the transfer of the data and that the third party that receives the data agrees to follow the privacy and security rules that the decision adopts below.

Finally, the Commission requires the utilities to file tariffs for connected HAN devices that are not "locked" to a third party and to provide customers

---

[76] There is a national effort to adopt standards for data exchange with the utility (a process called OpenADE – Open Automatic Data Exchange) and with the Smart Meter (a process called Smart Energy Profile) that will provide standardized and secure information. The Commission will consider via a regulatory proceeding whether to require California utilities to conform with these national standards when adopted.

[77] It is important to note that the privacy requirements adopted here do not apply to the Commission and its agents, including but not limited to contractors and consultants. SB 1476 creates obligations applicable to "electrical or gas corporation[s]." The Commission and its agents are subject to separate statutory provisions pertaining to the protection of data. These requirements are not the subject of this decision.

with information concerning the risks associated with misuse of energy usage data.

5. The CDT Recommendations Serve as a Starting Point for Consideration of Privacy and Security Rules to Protect Usage Data

The central privacy and security issues before the Commission in this proceeding are the determination of what privacy and security rules the Commission should adopt to protect usage data.

The most comprehensive efforts to address this question were the recommended rules offered by CDT and EFF to protect customer privacy interests, which are contained in Appendix A of their joint October 15, 2010 Response to the ACR.

As noted above, CDT, after discussion with several parties in the time leading to the October 25 and 26, 2010, workshops, presented revised recommended rules that became a focus of the workshops. CDT filed this revised proposal in its Reply Comments of November 12, 2010 as Appendix A-2 (and this is appended to this decision as Attachment C). In support of its recommendations, CDT stated:

> Our revised rule continues to reflect the Commission's decision, and the parties' broad general consensus, to implement the FIP principles. The revisions we have made reflect useful and constructive feedback from workshop discussions, including comments from PG&E, DRA, TURN, and other parties. More generally, our revised rule continues to reflect the goals of the Commission and parties to protect customer usage data, to bring order to the welter of regulations covering various aspects of the Smart Grid environment, and to accommodate and support innovation in technology and business practices. Importantly, the proposed rule fills gaps in the present framework—especially those gaps created by the inadequate and outdated "notice-and-choice"

> model of privacy protection—by using the full set of FIPs and "operationalizing" them for easy implementation by Smart Grid entities. [78]

The recommended rules of CDT played a central role in the development of the record in this proceeding. Most commenters focused on the CDT/EFF recommended rules and argued for acceptance, rejection or revision. The analysis that follows covers the record of this proceeding through discussing the rules recommended by CDT/EFF and the arguments of parties pertaining to each provision. Each section considers the rules recommended by CDT/EFF and adopts rules based on the record in this proceeding.

5.1. What Rules Should Determine Who is Covered, What Information is Covered, and Which Uses of Information are Primary?

CDT/EFF's recommended rules for protecting privacy and security of usage information begin with a set of definitions. These definitions are used throughout the recommended rules. The effect of these definitions is to determine to whom the recommended privacy rules apply and to determine the information covered by the recommended privacy rules.

The definitions also envision two categories of use for the usage information and recommend rules pertaining to each category to protect privacy of consumers and the security of the information. The two categories are: 1) Primary Purpose information – associated organically with the provision of utility services; and 2) All other uses of the information.

We begin our discussion of these recommended rules with a presentation of the CDT/EFF recommended definitions as contained in the CDT Reply

[78] CDT Reply Comments at 3.

Comments and then consider and adopt rules based on the record. The recommended definitions follow:

> **1. DEFINITIONS**
>
> (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].
>
> (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.
>
> (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 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.
>
> (d) **Secondary Purpose**. "Secondary purpose" means any purpose that is not a primary purpose.

In support of these recommended rules, CDT argued that "the Commission's jurisdiction includes, at a minimum, third parties that obtain

covered information under contract with or as an agent of a utility"[79] and that " the concept of 'obtaining covered information from a utility' encompasses entities that receive data from the meters (which is, after all, a utility-owned device)."[80] CDT argued that "it seems that the third parties taking data from the meter are doing so under agreement with the utility and thus should come under the jurisdiction of the Commission just as much as entities that receive data from a point further upstream in the utility's network."[81]

Concerning the definition of *primary purpose*, CDT argues that:

> … the distinction between *primary* and *secondary* purposes (Sections 1(c) and 1(d)) must be clear and must be maintained … Because primary purposes are excepted from the customer consent requirement, the Commission should take care not to enlarge this category to include any purposes that would leave customers vulnerable to unexpected or unknown collection, use, or disclosure of the highly revealing information that is covered by the rule. As such, uncontested ("primary") purposes must be tied directly to the provision of energy services and utility operations that have been approved by and subject to oversight by the Commission.[82]

CDT stressed that the distinction between primary and secondary purpose is an aspect of the proposed rules that "must not be revised."[83]

5.1.1. Position of Parties

PG&E supported the formulation of the definitions that CDT proposed. Of particular concern to PG&E was the clarification, incorporated in the above

[79] CDT Reply Comments at 11.

[80] *Id*.

[81] *Id*.

[82] *Id*. at 4-5.

[83] *Id*. at 4.

definitions, that Commission-authorized purposes constitute a "primary purpose."

SCE argued for the inclusion of words that define "customer." SCE would define customer as follows:

> **Customer.** For purposes of this rule, a "customer" is any individual, household, residence or business receiving retail generation, distribution or transmission service from an investor-owned utility.[84]

SCE then proposed revisions to substitute "customer" wherever the definition contains a litany of those whose usage information is subject to these rules. The net outcome of SCE's proposal was to leave the rules unchanged but to simplify their formulation.

TechNet and the State Privacy and Security Coalition raised cautionary notes, stating that

> The requirement that a specific purpose be indicated for each category of information collected and that the specific identity of third parties to which it is disclosed also be indicated suggests that relatively minor changes in services or products could trigger long notices that customer do not pay attention to, or repeated, annoying notice and consent requests to consumers. Requiring an entity to provide new notice every time it collaborates with another entity, for example, to provide an updated service or to begin to work with a new third party, even if the service to the customer is the same, appears unduly burdensome.[85]

TURN argued for the inclusion of gas aggregators in the covered entities, noting that "gas meters will be collecting and sending gas consumption data."[86]

---

[84] SCE Reply Comments at 3.

[85] TechNet and the State Privacy and Security Coalition Reply Comments at 6-7.

[86] TURN Reply Comments at 6.

In addition, TURN supported a broad interpretation of covered data, including "power quality data" which "may be relevant to promoting energy management solutions."[87]

SoCalGas, however, raised the fundamental question of whether non-electric utilities fall with the scope of this proceeding. SoCalGas stated:

> Although SoCalGas was in fact ordered [to] participate in this proceeding, SoCalGas wanted to raise a question of whether CDT/EFF's proposed definition matches the scope of this proceeding which to date seems to only be addressing the electric grid system. This is a fundamental question that the Commission must clarify before weighing the merits of CDT/EFF's proposed privacy policies and procedures. SoCalGas does not believe that the Commission has yet provided a clear direction that the policies being considered in this proceeding should be expanded beyond the electric grid system.[88]

5.1.2. Discussion

The definitions that determine the scope of the applicability of the rules recommended by CDT offer a reasonable starting place.

Some modifications, however, must be made before adopting the recommended rules.

There is substantial merit to SoCalGas's request that the Commission clarify whether this proceeding will adopt privacy rules affecting gas utilities.

Although the record of this proceeding makes it clear that the privacy issues that the Smart Meters raise are relevant for energy service providers, electrical corporations, gas corporations and community choice aggregators, the OIR initiating this proceeding defined a scope that now limits our work to issues

---

[87] *Id*.

[88] SoCalGas Reply Comments at 4-5.

affecting *electricity* provided by *electrical corporations* to their customers. Specifically, the OIR set the scope of this proceeding as follows:

> The general scope of this proceeding is to consider further actions, if needed, to comply with the requirements of EISA and also to consider policy and performance guidelines to enable the *electric utilities* to develop and implement a smart grid system in California.[89]

Since the initial phases of this proceeding were most relevant for the planning of PG&E, SCE, and SDG&E, the Commission, in D.09-07-039 excused PacifiCorp, Sierra Pacific Power, Bear Valley Electric Service and Mountain Utilities from participation in this proceeding.[90] Because the current scope of this proceeding applies to *PG&E, SCE, and SDG&E*, at this point it is not appropriate to adopt privacy rules for other companies without again modifying the scope of the proceeding and notifying potentially affected parties. For this reason, the definitions and regulations that we adopt will include a footnote to reflect that for now our rules apply only to *PG&E, SCE, and SDG&E*.

Since SB 1476, however, applies to gas corporations and to all electrical corporations, this decision modifies the scope of the proceeding and orders a separate new phase to consider whether the rules and policies adopted in this decision should apply to the remaining electrical corporations. In addition, community choice aggregators and electric service providers, should they use Smart Meters in the provision of service, will have exactly the same information that was the subject of the privacy protections adopted in this decision. Phase 2 of this proceeding will also explore whether the rules and policies adopted in this decision should also apply to community choice aggregators and electrical

[89] R.08-12-009 at 13, emphasis added.

[90] These utilities do not propose to install Smart Meters at this time.

service providers. The Commission will serve a copy of this decision on the remaining electrical corporations, gas corporations, community choice aggregators and electric service providers. These are listed in Attachment E to this order. Furthermore, the Commission will serve a copy of this decision on the service list in Rulemaking 10-05-005, a recent major gas industry proceeding.

In addition, the Commission exempts from privacy requirements those situations in which an individual or entity, with the consent of the consumer, receives usage information from a very small number of consumers. There is no need, for example, to regulate those situations in which a family member or friend takes care of the affairs of a small number of other people because of infirmity, age, or disability. This decision therefore exempts third parties obtaining information on ten or fewer households from all requirements, except for the requirement of obtaining the consumer's authorization for accessing usage data.

As noted in the jurisdictional discussion above, the Commission does not plan to regulate the consumer and what he or she determines to do with usage data. For this reason, these rules apply only to those third parties that obtain customer usage information directly from the utility or through a "locked" device that automatically delivers usage information from the smart meter to a third party without direction by the device owner.

SCE's proposal to add a definition of "customer" clarifies the rules that we adopt. This decision therefore adopts a definition of customer and modifies the definitions and rules recommended by CDT to refer to customers, rather than repetitively listing the different types of consumers protected by the rules.

Finally, to the extent the Commission itself seeks information to implement or review utility programs and practices, the Commission is not considered to be

a "Covered Entity" and that information is not considered to be "Covered Information" for the purposes of this decision. The Commission's access to customer information has its basis in statutes other than SB 1476. These statutes provide the Commission and its agents, including but not limited to contractors and consultants, with broad access to information in the possession of utilities.

To the extent other governmental organizations, such as the California Energy Commission or local governments, may seek Covered Information in a manner not provided in these rules, the Commission will determine such access in the context of the program for which information is being sought absent specific Legislative direction.

As revised, the definitions that the Commission finds reasonable and adopts are as follows:

> **1. DEFINITIONS**
>
> (a) **Covered Entity**. A "covered entity" is (1) any electrical corporation[91] or (2) any third party that collects, stores, uses, or discloses covered information relating to 11 or more customers who obtains this information from an electrical corporation or through the registration of a locked device that transfers information to that third party.[92]
>
> (b) **Customer.** For purposes of this rule, a "customer" is any entity receiving retail generation, distribution or transmission service from an electrical corporation.

---

[91] At this time "any electrical corporation" includes only PG&E, SCE, and SDG&E. Phase 2 of this proceeding will determine whether these rules should apply to gas corporations and other electrical corporations.

[92] The Commission and its agents, including but not limited to contractors and consultants, are not "covered entities" subject to these rules because the Commission and its agents are subject to separate statutory provisions pertaining to data. In addition, these rules do not apply at this time to gas corporations, other electrical corporations, community choice aggregators, or electric service providers. Phase 2 of this proceeding will make that determination.

(c) **Covered Information**. "Covered information" is any usage information obtained through the use of the capabilities of Advanced Metering Infrastructure when associated with any information that can reasonably be used to identify a customer, except that covered information does not include usage information from which identifying information has been removed such that a customer cannot reasonably be identified or re-identified. Covered information, however, does not include information provided to the Commission pursuant to its oversight responsibilities.

(d) **Primary Purposes**. The "primary purposes" for the collection, storage, use or disclosure of covered information are to—

(1) provide or bill for electrical power,

(2) fulfill other operational needs of the electrical system or grid,

(3) provide services as required by state or federal law or specifically authorized by an order of the Commission, or

(4) plan, implement, or evaluate demand response, energy management, or energy efficiency programs operated by, or on behalf of and under contract with, an electrical corporation.

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

5.2. What Rules Reasonably Promote the FIP Principle of Transparency?

The CDT recommended the following rules as a reasonable way to achieve the FIP principle of transparency:

2. TRANSPARENCY (NOTICE)

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

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

(c) **Form**. The notice shall be labeled "Privacy Policy: Notice of Collection, Storage, Use and Disclosure of Energy Usage Information" and shall—

(1) be written in easily understandable language, and

(2) be no longer than is necessary to convey the requisite information.

(d) **Content**. The notice shall state clearly—

(1) the identity of the covered entity,

(2) the effective date of the notice,

(3) the covered entity's process for altering the notice, including how the customer will be informed of any alterations, and where prior versions will be made available to customers, and

(4) the title and contact information, including email address, postal address, and telephone number, of an official at the covered entity who can assist the customer with privacy questions, concerns, or complaints regarding the collection, storage, use, or distribution of covered information.

5.2.1. Position of Parties on Recommended Rule to Promote Transparency

Concerning this recommended rule, PG&E supported adoption by the Commission without change.[93]

SCE provided comments recommending the replacement of the word "notice" with "notice or posted privacy policy" and provided extensive comments objecting to an earlier form of this proposed rule which implied that transactions and notice should be provided by paper. SCE objected to the extensive use of paper disclosures as costly, and inconsistent with the SCE policy to encourage the use of "on-line billing and notices as a means of cutting costs

[93] This conclusion is based on a review of PG&E's Reply Comments at Appendix A, page 6. PG&E recommends no revisions to the wording proposed by CDT.

and environmental waste associated with paper bills."[94] As an alternative, SCE argued that providing information at least twice a year on "how customers can view and obtain a copy of the covered entity's privacy policy on the collection, storage, usage and disclosure of energy usage data" offered a better approach.

Verizon, in the context of warning the Commission against the adoption of regulations that are "counterproductive, confusing and unduly burdensome,"[95] identified specific elements of this rule as unclear and burdensome. Specifically, Verizon argued that requiring an exact title "would result in a separate privacy policy for smart grid data for the vast majority of organizations that are not traditional electric utilities" and "would likely cause much confusion."[96] In addition, Verizon contended that it is not "clear by what standard the 'easily understandable language' requirement will be judged or enforced" and that "having multiple outdated notices be delivered to a consumer is wasteful, confusing, and in direct conflict with the need to provide easily understandable notice."[97]

TURN, like SCE, also objected to the focus on "paper" (rather than "electronic") communications that characterized an earlier draft of the CDT proposals.

---

[94] SCE Comments at 4.

[95] Verizon Reply Comments at 4.

[96] *Id*. at 4.

[97] *Id*. at 5.

5.2.2. Discussion: With Modifications, the Recommended Transparency Rule is Reasonable and Consistent with the Law; Paper is Not Necessary

The Transparency Rule recommended by CDT offers a reasonable approach to meeting the FIP goal of transparency, but requires modifications to improve its operation.

As CDT points out, it is important to provide information on privacy policy when confirming a new customer account and/or relationship. On the other hand, this need not be done by paper communication. In particular, the changes recommended by SCE to anticipate the growing use of electronic transactions are reasonable in light of the increasing importance of electronic transactions throughout the economy.

Verizon's argument that there is no need to specify the exact title of the document containing the Smart Grid privacy policy is reasonable. As Verizon points out, it makes no sense to create a separate "Smart Grid privacy page" separate from other privacy pages. A separate page on the Smart Grid may confuse customers concerned with privacy.

On the other hand, Verizon's argument that the standard of "reasonably understandable" will be difficult to enforce is not convincing. Much utility regulation relies on a reasonableness standard and the record in this proceeding does not support the adoption of another standard.

Finally, although there is no need to provide customers with prior versions of the privacy policies, we conclude that they should remain available for customers who desire them, but that they need not be routinely displayed.

This decision finds reasonable and adopts the following transparency rule:

2. TRANSPARENCY (NOTICE)

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

(b) **When Provided**. Covered entities shall provide written or electronic notice when confirming a new customer account and at least twice a year informing customers how they may obtain a copy of the covered entity's privacy policy regarding the collection, storage, use, and disclosure of covered information, and shall provide conspicuous posting of the notice and privacy policy or link to the notice and privacy policy on the home page of their website, and shall include a link to their notice and privacy policy in all electronic correspondence to customers.

(c) **Form**. The notice shall be labeled to make clear that it is a privacy notice and the notice shall communicate where a consumer may find policies affecting the collection, storage, use and disclosure of energy usage information and shall—

(1) be written in easily understandable language, and

(2) be no longer than is necessary to convey the requisite information.

(d) **Content.** The notice and the posted privacy policy shall state clearly—

(1) the identity of the covered entity,

(2) the effective date of the notice or posted privacy policy,

(3) the covered entity's process for altering the notice or posted privacy policy, including how the customer will be informed of any alterations, and where prior versions will be made available to customers, and

(4) the title and contact information, including email address, postal address, and telephone number, of an official at the covered entity who can assist the customer with privacy questions, concerns, or complaints regarding the collection, storage, use, or distribution of covered information.

5.3. What Rule Best Operationalizes the FIP Principle of Specifying the Purpose for Collecting or Disclosing Information?

The CDT recommends the following rule to achieve the FIP principle of insuring that the data is collected to serve a clear and specific purpose:

> **3. PURPOSE SPECIFICATION**
>
> The notice required under section 2 shall provide—
>
> (a) an explicit description of—
>
> (1) each category of covered information collected, used, stored or disclosed by the covered entity, and, for each category of covered information, the reasonably specific purposes for which it will be collected, stored, used, or disclosed, and
>
> (2) each category of covered information that is disclosed to third parties, and, for each such category, (i) the purposes for which it is disclosed, and (ii) the identities of the third parties to which it is disclosed;
>
> (b) the periods of time that covered information is retained by the covered entity;
>
> (c) a description of—
>
> (1) the means by which customers may view, inquire about, or dispute their covered information, and
>
> (2) the means, if any, by which customers may limit the collection, use, storage or disclosure of covered information and the consequences to customers if they exercise such limits.

CDT argued that "[t]he purpose specification is the linchpin of the proposed rules … If purposes are not specifically described, the other elements of the rule become meaningless."[98]

5.3.1. Positions of Parties on Purpose Specification

PG&E, although generally supportive of the CDT proposal, argued that the requirement to disclose the identify of all companies receiving information,

[98] CDT Reply Comments at 5-6.

as 3(a)(2) requires, is not reasonable. PG&E explained that "PG&E contracts with hundreds of third parties for the purposes of operating its utility system and providing utility services to customers, and thus providing the identity of each and every contractor with whom it shares covered information for utility operational purposes is commercially unreasonable."[99] PG&E, although opposing an automatic disclosure of each contractor's identity, noted that the "Commission retains the discretion to request the identity of each contractor from utilities as part of normal regulatory oversight."[100]

SCE, similarly to PG&E, claimed that it also uses a large number of contractors and that a requirement to disclose all third parties would be "overly burdensome and costly."[101] SCE argued that disclosing the *categories* of companies receiving the information, rather than the *identities*, would provide adequate information to the consumers while being less burdensome.

TechNet and the State Privacy and Security Coalition raised cautionary notes pertaining to CDT's recommended regulation, stating that:

> The requirement that a specific purpose be indicated for each category of information collected and that the specific identity of third parties to which it is disclosed also be indicated suggests that relatively minor changes in services or products could trigger long notices that customer do not pay attention to, or repeated, annoying notice and consent requests to consumers. Requiring an entity to provide new notice every time it collaborates with another entity, for example, to provide an updated service or to begin to work with a

[99] PG&E Reply Comments at 6.

[100] *Id*.

[101] SCE Reply Comments at 5.

> new third party, even if the service to the customer is the same, appears unduly burdensome.[102]

Verizon also claimed that such a policy would be "incredibly burdensome to implement and result in repeated changes to a privacy policy."[103]

5.3.2. Discussion: Recommended Rule with Revisions can Meet FIP Goal with Reduced Regulatory Burdens and Less Potential Consumer Confusion

The recommended rule whereby the notice to customers states the purpose for which the data is collected is a reasonable approach to operationalizing the FIP principle of specifying the purpose for collecting or disclosing information, but some changes are needed in light of the immense scope and complexity of utility operations.

PG&E, TechNet and the State Privacy and Security Coalition, and Verizon argue persuasively that the recommended disclosure of the identities of *all* companies receiving information is not a reasonable requirement because of the large and changing number of companies that assist a utility in its operations. Not only would such a requirement prove burdensome, but the multiple notices that current operations would require may confuse consumers and lead to a barrage of communications.

It is, however, reasonable for the Commission to hold a utility responsible for assuring that all companies assisting the utility in its utility operations comply with privacy rules adopted by the Commission. Since the Commission can always obtain access to the names of the companies receiving data and the utility is responsible for the conduct of the firms with which it contracts, the

---

[102] TechNet and the State Privacy and Security Coalition Reply Comments as 6-7.

[103] Verizon Reply Comments at 4.

Commission does not need to require automatic disclosure of the names of all the companies receiving information.

SCE argued persuasively that providing information on the *categories of companies* receiving information provides sufficient information to customers about the potential uses of their information. Such an approach is consistent with the spirit of the FIP principles because it will inform customers without deluging the customers with information.

Once again, this decision makes it clear that it will remain the responsibility of utilities to ensure that companies supporting utilities in utility operations follow the same rules as the utility itself and do not use the information for any purpose other than that for which the utility had contracted their services. This requirement, along with the Commission's ability to obtain the names of all companies receiving usage data, makes the disclosure of individual company names unnecessary for protecting customer interests. Moreover, by only requiring the disclosure of the categories of companies to whom data is disclosed, the utilities and consumers will avoid the burdensome and frequent notices that disclosure of minor changes in services, products, or vendors would require.

For the reasons outlined above, it is reasonable to adopt a rule pertaining to the disclosure of the specific purposes for which the information is collected as follows:

> **3. PURPOSE SPECIFICATION**
> The notice required under section 2 shall provide—
> (a) an explicit description of—
> (1) each category of covered information collected, used, stored or disclosed by the covered entity, and, for each category of covered information, the reasonably specific purposes for which it will be collected, stored, used, or disclosed, and

(2) each category of covered information that is disclosed to third parties, and, for each such category, (i) the purposes for which it is disclosed, and (ii) the number and categories of third parties to which it is disclosed;

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

(c) a description of—

(1) the means by which customers may view, inquire about, or dispute their covered information, and

(2) the means, if any, by which customers may limit the collection, use, storage or disclosure of covered information and the consequences to customers if they exercise such limits.

5.4. What Rules Reasonably Promote the FIP Principle of Individual Access and Control of Smart Meter Data?

The CDT recommended that the Commission adopt the following rules to achieve the FIP principle of individual participation in the privacy and control of data:

4. INDIVIDUAL PARTICIPATION (ACCESS AND CONTROL)

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

(1) in an easily readable format that is at a level no less detailed than that at which the covered entity discloses the data to third parties.

(2) The Commission shall, by subsequent rule, prescribe what is a reasonable time for responding to customer requests for access.

(b) **Control**. Covered entities shall provide customers with convenient mechanisms for—

(1) granting and revoking authorization for secondary uses of covered information,

(2) disputing the accuracy or completeness of covered information that the covered entity is storing or distributing for any primary or secondary purpose, and

(3) requesting corrections or amendments to covered information that the covered entity is collecting, storing, using, or distributing for any primary or secondary purpose.

(c) **Disclosure Pursuant to Legal Process**.

(1) Except as otherwise provided in this rule or expressly authorized by state or federal law or by order of the Commission, a covered entity shall not disclose covered information except pursuant to a warrant or other court order naming with specificity the customers whose information is sought. Unless otherwise directed by a court, law, or order of the Commission, covered entities shall treat requests for real-time access to covered information as wiretaps, requiring approval under the federal or state wiretap law as necessary.

(2) Unless otherwise prohibited by court order, law, or order of the Commission, a covered entity, upon receipt of a demand for disclosure of covered information pursuant to legal process, shall, prior to complying, notify the customer in writing and allow the customer 7 days to appear and contest the claim of the person or entity seeking disclosure.

(3) Nothing in this rule prevents a person or entity seeking covered information from demanding such information from the customer under any applicable legal procedure or authority.

(4) Nothing in this section prohibits a covered entity from disclosing covered information with the consent of the customer, where the consent is express, written and specific to the purpose and to the person or entity seeking the information.

(5) Nothing in this rule prevents a covered entity from disclosing, in response to a subpoena, the name, address and other contact information regarding a customer.

(6) On an annual basis, covered entities shall report to the Commission the number of times that customer data has

> been sought pursuant to legal process without customer consent, and for each such instance, whether it was a civil or criminal case, whether the covered entity complied with the request as initially presented or as modified in form or scope, and how many customers' records were disclosed. The Commission may require the covered entity to make such reports publicly available without identifying the affected customers, unless making such reports public is prohibited by state or federal law or by order of the Commission.

5.4.1. Position of Parties

On this particular rule recommended by CDT, PG&E noted that it had proffered several revisions to ensure that the access and control conforms to common legal practices of the Commission and courts regarding access to information. CDT incorporated PG&E's proposed changes into text before filing its Reply with the Commission, and PG&E had no further comments on this rule.

SCE objected to 4(c)(2) above, which requires customer notification in writing and allowing the customer seven days to appear and contest the disclosure. SCE argued that this practice "exceeds current requirements for the IOUs under law and Commission order, and would place the IOUs in a position of possibly interfering with law enforcement activities."[104] SCE provided a compelling example that suggests that the rule recommended by CDT is too broad:

> For example, Section 588 of the Public Utilities Code allows the district attorney to access customer confidential information (except usage information) from public utilities in child abduction cases. Nothing in Section 588 *prohibits* an IOU from notifying the customer whose information is sought in advance of the mandatory

[104] SCE Reply Comments at 6.

> disclosure; yet doing so may interfere with the district attorney's efforts to locate and recover an abducted child.[105]

SCE argued that it is clear that in a situation such as this, when time and confidentiality are both critical, to delay the release of information and to provide customer notice of a potential disclosure of information would be inconsistent with the intent of the law granting the district attorney this authority in these cases. SCE recommended that the Commission, when adopting a rule on this issue, delete requirement 4(c)(2).

SCE also argued that the recommended annual reporting requirement, contained in 4(c)(6) is "overly burdensome, costly to comply with, and unnecessary because the Commission can request this information at any time from the IOUs and other entities over whom the Commission has jurisdiction for consumer protection purposes…"[106] SCE then recommended a reformulation of the recommended rules to read:

> 4(c)(6) Upon request of the Commission, covered entities shall report to the Commission on disclosures of covered information made pursuant to legal process. The Commission may make such reports publicly available without identifying the affected customers, unless making such reports public is prohibited by state or federal law or by order of the Commission.[107]

---

[105] *Id*.

[106] *Id*. at 7.

[107] *Id*.

5.4.2. Discussion: Recommended Rules Provide a Reasonable Approach to Providing Customer with Access and Control of Usage Data, but Modifications Are Warranted

The rules recommended by CDT provide a reasonable approach to providing a customer with access to usage data and control of that usage data.

Some modifications, however, are warranted in the rules recommended pertaining to disclosures made pursuant to a legal process to ensure that the adopted rule contains the flexibility needed to address the range of situations that can occur.

In particular, SCE's criticism of requirement 4(c)(2), which would require the advance notice of a request by an authority for any access to data, is well taken. As SCE's example makes clear, the proposed rule lacks the flexibility to address extreme cases, such as the child abduction scenario hypothesized. Such advance notice, however, is clearly warranted in the case of a subpoena, and 4(c)(2) is therefore modified to require advance notice only in the case when a subpoena demanding information concerning a customer is served on the utility.

Similarly, SCE's recommendation to change the reporting requirement from a mandated annual report to one that would be prepared only upon the request of the Commission is also reasonable. As a regulatory agency that receives a large number of reports, the Commission's experience indicates that unless there is an audience within the Commission or the larger community representing consumers which wants the information contained in a specific report, the reports can quickly exceed the ability of either the Commission or consumer representatives to process information. Since no party has stated an explicit need for this particular report, the Commission declines to require its submission.

In addition, since this decision (below) orders PG&E, SCE, and SDG&E to file advice letters containing revised tariffs to provide wider access to covered data, there is no need to include paragraph 4(a)(2), which promises future Commission action.

Finally, § 2891(d)(5), which sets out rules to protect the privacy of telephone customers, specifically does not apply to "[i]nformation provided to an emergency service agency responding to a 911 telephone call or any other call communicating an imminent threat to life or property."[108] Since smart meters may be able to communicate information that may indicate an imminent threat to life or property, such as the fact of a gas leak or an electric short, prudence dictates that the Commission should adopt a similar stance towards this information.

This decision finds reasonable and adopts this rule as follows:

> **4. INDIVIDUAL PARTICIPATION (ACCESS AND CONTROL)**
>
> (a) **Access**. Covered entities shall provide to customers upon request convenient and secure access to their covered information in an easily readable format that is at a level no less detailed than that at which the covered entity discloses the data to third parties.
>
> (b) **Control**. Covered entities shall provide customers with convenient mechanisms for—
>
> (1) granting and revoking authorization for secondary uses of covered information,
>
> (2) disputing the accuracy or completeness of covered information that the covered entity is storing or distributing for any primary or secondary purpose, and
>
> (3) requesting corrections or amendments to covered information that the covered entity is collecting, storing, using, or distributing for any primary or secondary purpose.

[108] Section 2891(d)(5).

(c) **Disclosure Pursuant to Legal Process**.

(1) Except as otherwise provided in this rule or expressly authorized by state or federal law or by order of the Commission, a covered entity shall not disclose covered information except pursuant to a warrant or other court order naming with specificity the customers whose information is sought. Unless otherwise directed by a court, law, or order of the Commission, covered entities shall treat requests for real-time access to covered information as wiretaps, requiring approval under the federal or state wiretap law as necessary.

(2) Unless otherwise prohibited by court order, law, or order of the Commission, a covered entity, upon receipt of a subpoena for disclosure of covered information pursuant to legal process, shall, prior to complying, notify the customer in writing and allow the customer 7 days to appear and contest the claim of the person or entity seeking disclosure.

(3) Nothing in this rule prevents a person or entity seeking covered information from demanding such information from the customer under any applicable legal procedure or authority.

(4) Nothing in this section prohibits a covered entity from disclosing covered information with the consent of the customer, where the consent is express, in written or electronic form, and specific to the purpose and to the person or entity seeking the information.

(5) Nothing in this rule prevents a covered entity from disclosing, in response to a subpoena, the name, address and other contact information regarding a customer.

(6) Upon request of the Commission, covered entities shall report to the Commission on disclosures of covered information made pursuant to legal process. The Commission may make such reports publicly available without identifying the affected customers, unless making such reports public is prohibited by state or federal law or by order of the Commission.

(d) **Disclosure of Information in Situations of Imminent Threat to Life or Property.** These rules concerning access, control and disclosure do not apply to information provided to emergency responders in situations involving an imminent threat to life or property.

5.5. What Rules Reasonably Promote the FIP Principle of Data Minimization?

Data minimization is one of the key FIP principles, and the CDT has recommended the following rules pertaining to data minimization to the Commission for adoption:

5. DATA MINIMIZATION

(a) **Generally**. Covered entities shall collect, store, use, and disclose only as much covered information as is reasonably necessary or as authorized by the Commission to accomplish a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

(b) **Data Retention**. Covered entities shall maintain covered information only for as long as reasonably necessary or as authorized by the Commission to accomplish a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

(c) **Data Disclosure**. Covered entities shall not disclose to any third party more covered information than is reasonably necessary or as authorized by the Commission to carry out on behalf of the covered entity a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

In support of these recommended rules, CDT argued that:

… data minimization is a powerful tool for protecting against security and privacy threats. It is a basic security "best practice" that customers will and should be able to expect of any entity using revealing covered information. Moreover, in light of many recent high-profile breaches of sensitive consumer data, customer confidence that Smart Grid technologies and business practices

> employ sufficient privacy and security practices will be key to the growth and development of the Smart Grid marketplace.[109]

5.5.1. Positions of Parties on Data Minimization

The principle of data minimization generated much comment. PG&E argued that:

> PG&E agrees with the general goal of minimizing the scope and retention of covered information, but this goal should be balanced against the need by the Commission and utilities to maintain records and data for operational and policy purposes, such as resolution of customer billing disputes; energy policy planning and analysis; and cost of service review authorized by the Commission.[110]

UCAN supported a data minimization strategy with a few caveats. UCAN argued:

> … the potential for privacy to be compromised is minimized if the amount of personal and household information that is captured and retained by the utility and third-parties is limited. Data retention is an important subset of this issue. Personal information that is collected via Smart Grid systems should be retained only as long as needed for the purposes identified by the consumer.[111]

SDG&E, on the other hand, in addition to its general opposition to CDT's recommendations, detailed its opposition to the principle of data minimization. SDG&E argued:

> ... the [proposed regulatory] scheme requires further analysis in order to achieve greater consistency in provisions and reasonably [sic] accommodation before the CPUC considers establishing electric utility operational FIPs. For example, SDG&E finds that the recommendation for implementation of the "Data Minimization Principle" requires further party and stakeholder discussion in order

[109] CDT Reply Comments at 7, footnotes omitted.

[110] PG&E Reply Comments at 8.

[111] UCAN Reply Comments at 5.

> to fit the business needs of the electric utilities existing and potentially [sic] future operations. In addition, terminology used in the CDT & EFF proposal such as "shall" and "reasonable" is extremely vague, expression application is too broad, and the language may be subject to a variety of interpretations.[112]

AT&T also opposed CDT's data retention requirements. AT&T contended:

> The data retention requirements are both too limiting and too vague. It proposes energy usage information be kept "only for as long as necessary…" It is unclear under this standard whether a company that maintains Smart Grid data for 2 years could be liable for maintaining the data too long if its competitor maintains the same data for only 1 year. Moreover, it would seem to preclude Smart Grid applications that rely on several years of historical data.[113]

TechNet and the State Privacy and Security Coalition (filing jointly) similarly argued that "the Commission should not impose a binding data minimization requirement."[114] Specifically, TechNet and the State Privacy and Security Coalition objected to an earlier formulation by CDT of this requirement that lacked the word "reasonably" and appeared to impose both a requirement and a liability on any company that collected data that was not absolutely "necessary." TechNet and the State Privacy and Security Coalition also argued that "data minimization provisions were rejected by the Legislature on multiple occasions" and then proceeded to cite from the legislative history of SB 837.[115]

---

[112] SDG&E Reply Comments at 5.

[113] AT&T Reply Comments at 1.

[114] TechNet and the State Privacy and Security Coalition Reply Comments at 7.

[115] *Id*. at 8.

5.5.2. Discussion: Data Minimization Requirement is Reasonable

In reply comments, CDT incorporated major changes that resolve many of the defects in this recommended rule. As revised by CDT in its reply comments, the recommended rule is reasonable and we adopt this rule.

Adopting this rule is reasonable because data minimization promotes privacy and security by limiting the amount of personal data collected and the amount that must be secured and protected. As such, it offers a practical strategy for protecting sensitive information. Thus, a principle of data minimization should guide the development of utility and regulatory policies towards data.

Adopting a principle of data minimization will, however, constitute a new approach to regulatory oversight for both utilities and this Commission. The data historically collected by the Commission and by utilities most commonly concerned the information needed to ensure that rates were reasonable and service reliable. The information collected commonly included such items as company costs, aggregate demand, and company revenues. Little data collected or available would disclose the daily activities of individual utility customers.

There is, however, a natural tension between a data minimization rule and current practices regarding utility information. The endorsement of a principle of "data minimization" will serve as a guide for the revision of other regulations in specific regulatory proceedings. Adopting a principle of "data minimization" does not change any regulations that currently require the retention of data for periods of time nor does it change any specific reporting requirements. Moreover, it does not preclude any Commission requests for information. Still, the Commission adopts this principle to signal our interest in incorporating this strategy into our program to protect consumer privacy and to keep data secure.

The revisions to the recommended rules incorporated by CDT in Reply Comments now cause these rules to conform to the realities of Commission regulation. As revised, the regulation permits the retention of as much information as "is reasonably necessary" and for as long as is "reasonably necessary." In addition, the rules now formally recognize the role of the Commission in creating data collection and retention requirements through inclusion of the words "as authorized by the Commission" in the formulation of this requirement.

As revised, this recommended rule creates no new liability that would fall upon utilities and other entities in conjunction with data retention. Instead, these rules make clear that as a utility proposes to collect personal information, it should propose for consideration by this Commission both limitations on the amount of personal information collected and the time period for data retention.

Finally, no further study of this requirement is warranted. As the discussion above has made clear, the privacy protection provisions are closely tied to SB 1476 (not SB 837, which TechNet and the State Privacy Coalition cite but fail to note never became law.[116]) Although SB 1476 does not include a requirement for data minimization or a limitation on data retention, the practical role that a principle of data minimization plays as a "best practice" in a data privacy and security strategy make it consistent with both the goals of SB 1476 and the Pub. Util. Code.

[116] TechNet and the State Privacy Coalition Reply Comments at 8-9.

5.6. What Use and Disclosure Limitations Reasonably Protect Consumers Yet Permit the Authorized Use and Disclosure of Electricity Consumption Information?

The heart of any privacy program is the limitations placed on the use and disclosure of the information that the program seeks to protect. CDT recommended the following rules to protect energy usage data in its Reply Comments, and they once again serve as a good starting point for our discussion.

> **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. Other covered entities may collect, store and use covered information only with prior customer consent, except as otherwise provided here.
>
> (c) **Disclosures to Third Parties**.
>
> (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.
>
> (2) **Subsequent Disclosures**. Any entity that receives covered information derived initially from a gas or electrical

corporation, electric service provider or community choice aggregator may disclose such covered information to another entity without customer consent for a primary purpose, provided that the entity disclosing the covered information shall, by contract, require the entity receiving the covered information to use the covered information only for such primary purpose and to agree to store, use, and disclose the covered information under policies, practices and notification requirements no less protective than those under which the gas or electrical corporation, electric service provider or community choice aggregator from which the covered information was initially derived itself operates as required by this rule.

(3) **Terminating Disclosures to Entities Failing to Comply With Their Privacy Assurances**. When an entity discloses covered information to any other entity under this subsection 6(c), it shall specify by contract that it shall be considered a material breach if the receiving entity engages in a pattern or practice of storing, using or disclosing the covered information in violation of the receiving entity's commitment to handle the covered information under policies no less protective than those under which the gas or electrical corporation, electric service provider or community choice aggregator from which the covered information was initially derived itself operates in compliance with this rule. If an entity disclosing covered information finds that an entity to which it disclosed covered information is engaged in a pattern or practice of storing, using or disclosing covered information in violation of the receiving entity's privacy and data security commitments related to handling covered information, the disclosing entity shall cease disclosing covered information to such receiving entity.

(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) authorized by the Commission pursuant to its jurisdiction and control.

(e) **Customer Authorization**.

(1) Authorization. Separate authorization by each customer must be obtained for each secondary purpose.

(2) Revocation. Customers have the right to revoke, at any time, any previously granted authorization.

(3) Expiration. Customer consent shall be deemed to expire after two years, after which time customers will need to reauthorize any secondary purposes.

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

In support of these recommended rules, CDT argued that where "the provision of the [utility] service and the collection, storage and use of the information are so inextricably intertwined …consent could not realistically be withheld" and therefore "a provider … [of electric service] should not have to obtain customer consent to collect, store or use energy information in the course of providing the energy service."[117] CDT also contended that "[w]here data … is disclosed to third parties for use in providing energy-related services on behalf of and under contract with the utility …, prior customer consent is not needed … for the disclosure."[118]

CDT, however, argued that disclosure to other parties is far different, and "[w]hen covered information is collected by or flows to entities that are not

[117] CDT Reply Comments at 15-16.

[118] *Id*.

utilities and is being used for purposes … other than providing services under contract with a utility, prior consent must be obtained" [119] because such a requirement is consistent with "customer expectations."[120]

Finally, CDT argued that its "chain of responsibility" proposal, contained in 6(c)(3), is key to Commission enforcement of its privacy regulations. CDT describes its "chain of responsibility" as "a concept widely accepted in the commercial sphere: a contractual chain of downstream responsibility, in which the party at the top of the stream has the right to insist that its next immediate downstream partner abides by privacy rules … and so on."[121]

5.6.1. Positions of Parties

PG&E objected to the "chain of downstream responsibility" concept. PG&E argued that:

> … as a matter of public policy and practical implementation, PG&E does not recommend that utilities or their third party contractors or agents be required to enforce these privacy principles through the indirect means of commercial lawsuits or civil action for breach of contract. PG&E also does not recommend that such parties be required to directly register or be certified by the Commission because the benefit of such third party certification is likely to be offset by the deterrence of third parties from developing and providing new products and services to customers using covered information in a manner consistent with privacy rules already applicable to all entities under general law.[122]

SCE was similarly skeptical about the rules pertaining to the "chain of downstream responsibility" pertaining to disclosures. In addition, SCE

---

[119] *Id*.

[120] *Id*. at 16.

[121] *Id*. at 18.

[122] PG&E Reply Comments at 10.

recommended the use of the words "covered entity" and "third party" in part to address the question of whether energy service providers or gas utilities have received proper notice that these privacy rules could apply to these companies with minor changes.

TechNet and the State Privacy and Security Coalition objected to the automatic expiration of a customer's consent to the provision of data for a secondary purpose. TechNet and the State Privacy and Security Coalition argued:

> Customers who have signed up for a service and continue to expect to receive it face potential interruption of service if they do not provide consent. Companies will face significant costs to keep track of, notify and obtain consent from a constantly evolving customer database. Even for a large company, this is burdensome and costly. For a small company, this is an onerous expense, potentially diverting resources away from research and development.[123]

Verizon similarly argued against the expiration rule, contending:

> Consumer expect that the choices they make regarding their data use preferences remain in effect until and unless they change them, and they should have the option to make changes at any time they choose. However, requiring an arbitrary expiration of consumer consent after a two-year period is neither beneficial or convenient to consumers and should not be adopted.[124]

AT&T also made a similar argument against the automatic expiration rule, and argued further that the customer authorization requirements are "too prescriptive"[125] and "unnecessary and burdensome to the customer." [126] Instead,

---

[123] TechNet and the State Privacy and Security Coalition Reply Comments at 9.

[124] Verizon Reply Comments at 5.

[125] AT&T Reply Comments at 1.

[126] *Id*. at 2.

AT&T argued that "[a] less burdensome way to accomplish the same goal would be for providers to remind customers every two years that they may change or revoke their privacy selections at any time."[127]

EnerNOC also argued that "the two-year sunset on authorization to share data recommended by TURN and DRA is inappropriate for CI&I customers."[128] EnerNOC stated that "CI&I customers typically sign contracts that require the provision of energy usage data to implement … For these customers, authorization to share their data should coincide with the term of their contract."[129]

Concerning the issue of disclosure for a secondary purpose, TURN recommended "that the language should be simplified to state that disclosure to any third party who is not under contract with the utility is prohibited absent explicit customer authorization."[130]

DRA proposed narrower limits on the disclosure of energy usage data, and argued that "[s]ince the Smart Grid is intended to save energy, increase electricity reliability and reduce greenhouse gases, allowed uses should be limited to these same purposes."[131] DRA also argued for a limited interpretation of "primary purpose," and argued that primary purpose "should be limited to activities necessary to provide basic electric service."[132]

---

[127] *Id*. at 2.

[128] EnerNOC Reply Comments at 5.

[129] *Id*.

[130] TURN Reply Comments.

[131] DRA Reply Comments at 9.

[132] *Id*. at 10.

5.6.2. Discussion: Enforcement Critical to Privacy Rules

The "chain of responsibility" approach to protecting privacy and enforcing policy rules is a reasonable approach to enforcement. This decision therefore declines requests by PG&E and SCE to not adopt this approach. As many parties have pointed out, ensuring compliance with privacy policies is a key element of an effective privacy policy. Electric utilities are already responsible for the protection of customer privacy whenever they use a third party to perform utility operations. The "chain of responsibility" currently works in these contractual relationships. It currently provides a reasonable approach to the protection of customer privacy and it can continue to do so.

Although the Commission sees demand response, energy management and energy efficiency to be primary purposes, it is reasonable to permit customers to opt out of disclosure of usage data to third parties, unless otherwise directed by the Commission. Even if disclosed to a third party, the information is still subject to the protections that apply to the utility, and should only be disclosed pursuant to a contract that ensures compliance with privacy and security measures, as SB 1476 requires.

In addition, to the extent customer usage information becomes available to consumers and third parties pursuant to utility tariffs, rather than contracts, the tariffs can require that customers demonstrate that they have authorized the transfer of information. In additions, the tariffs can permit a customer to withdraw the authorization at any time. Finally, when a third party does not comply with tariff requirements to protect the privacy and security of data, the Commission can order the utility to notify customers and can order the utility to stop providing the third party with data. In addition to cutting off the provision of data on current customers, the Commission can also make the third party

ineligible to obtain customer usage information from the utility in the future. These sanctions can be written into the tariff and/or considered by the Commission in the course of a proceeding.

The request of SCE for using the words "covered entity" and "third party" is reasonable. At this time, rules that this decision adopts apply only to the three electric utilities – PG&E, SCE, and SDG&E – and to third parties who gain access to this usage data. This formulation, nevertheless, recognizes that the Commission has not provided electric service providers, community choice aggregators, other electrical corporations, or gas corporations with notice that the rules and policies adopted in this decision could apply to them and permits ready extension to these entities should the Commission, after a proceeding undertaken for this purpose, elect to do so.

There is merit in the arguments of TechNet and the State Privacy and Security Coalition, Verizon and AT&T that an automatic expiration of disclosure authority after two years is not in the customer interest and would be burdensome to the customer. This decision concludes that an automatic expiration of an authorization is not reasonable. Instead, this decision adopts a requirement that a covered entity to whom usage information for a non-primary purpose is disclosed must provide an annual reminder of the prior authorization along with an opportunity to opt out. This requirement offers a reasonable approach to ensure that customers continue to have control over the disclosure of their usage information.

EnerNOC's comments raise important issues concerning contractual arrangements involving commercial, industrial, and institutional (CII) customers. This decision revises CDT's recommended rules concerning disclosure to ensure that they do not undermine contractual arrangements with non-residential

customers. The disclosure rules that this decision adopts permit non-residential customers to agree to disclose usage information pursuant to the terms of any commercial contract of finite duration without the right to cancel at any time. This decision, however, maintains the right of residential customers and other non-residential customers to rescind authorization of disclosure at any time.

Concerning TURN's request for clarifying language, the language that this decision adopts achieves the clarification that TURN desires – no disclosure for a secondary purpose would be permitted without consumer authorization.

Concerning DRA's request that the Commission prohibit disclosure for secondary purposes beyond those related to energy policies, this decision declines to adopt this policy for several reasons. First, the consumer should have control of his or her data, and restricting the consumer's ability to disclose this data is inconsistent with our view of consumer sovereignty. Second, limiting disclosure to only those purposes related to energy policies would be burdensome to both the consumer and the Commission. In particular, a number of purposes – such as the marketing of efficient appliances or software applications – would require a Commission determination of whether they are "eligible" for disclosure because they involve a mixture of profit-oriented marketing combined with energy efficiency concerns. If the regulatory process must sort its way through each of these uses of consumption data to determine whether it is an "eligible" purpose, the regulatory reviews will have a chilling effect on innovation and will impose a burden on the regulatory process by consuming resources better used to protect consumers who are harmed.

Furthermore, in reviewing the recommended exceptions to the prior authorization requirement for disclosures for secondary purposes contained in 6(d), this decision adopts the language "pursuant to legal process" contained in

4(d) above. This formulation clearly embraces "law enforcement pursuant to legal process." In addition, it is also reasonable and prudent to create an exception to this requirement in situations where there is an imminent threat to life or property, as was done in 4(d) above.

Finally, we also note that SB 1476 allows an electric or gas utility to use aggregated consumption data, provided that "all information has been removed regarding the individual identity of a customer."[133] Furthermore, we note that Pub. Util. Code § 394.4(a) allows electric service providers to release customer data on an aggregated level as long as that the release of the information does not reveal customer specific information. As a result, this decision affirms that the availability and use of aggregated data, with all personally identifiable information removed, is consistent with the terms of Pub. Util. Code §§ 8380 and 394.4(a) and does not require the authorization of the customer.

Based on these considerations, this decision finds reasonable and adopts the following 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 electrical corporation may collect, store and use covered information for primary purposes without customer consent. Other covered entities may collect, store and use covered information only with prior customer consent, except as otherwise provided here.

(c) **Disclosures to Third Parties**.

(1) **Initial Disclosure by a Covered Entity**. A covered entity may disclose covered information to a third party without

[133] Pub. Util. Code § 8380(e)(1).

customer consent when explicitly ordered to do so by the Commission or 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 consistent with applicable program terms and conditions, unless otherwise directed by the Commission.

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

(3) **Terminating Disclosures to Entities Failing to Comply With Their Privacy Assurances**. When a covered entity discloses covered information to a third party under this subsection 6(c), it shall specify by contract that it shall be considered a material breach if the third party engages in a pattern or practice of storing, using or disclosing the covered information in violation of the third party's contractual obligations to handle the covered information under policies no less protective than those under which the covered entity from which the covered information was initially derived operates in compliance with this rule. If a covered entity disclosing covered information finds that a third party to

which it disclosed covered information is engaged in a pattern or practice of storing, using or disclosing covered information in violation of the third party's contractual obligations related to handling covered information, the disclosing entity shall promptly cease disclosing covered information to such third party.

(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. This authorization is not required when information is—

(1) provided pursuant to a legal process as described in 4(c) above;

(2) provided in situations of imminent threat to life or property as described in 4(d) above; or

(3) authorized by the Commission pursuant to its jurisdiction and control.

(e) **Customer Authorization**.

(1) **Authorization**. Separate authorization by each customer must be obtained for each secondary purpose.

(2) **Revocation**. Customers have the right to revoke, at any time, any previously granted authorization. Non-residential customers shall have the same right to revoke, unless specified otherwise in a contract of finite duration.

(3) **Opportunity to Revoke**. The consent of a residential customer shall continue without expiration, but an entity receiving information pursuant to a residential customer's authorization shall contact the customer, at least annually, to inform the customer of the authorization granted and to provide an opportunity for revocation. The consent of a non-residential customer shall continue in the same way, unless specified otherwise in a contract of finite duration, but an entity receiving information pursuant to a non-residential customer's authorization shall contact the customer, to inform the customer of the authorization granted and to provide an opportunity for revocation either upon the

termination of the contract, or annually if there is no contract..

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

(g) **Availability of Aggregated Usage Data**. Covered entities shall permit the use of aggregated usage data that is removed of all personally-identifiable information to be used for analysis, reporting or program management provided that the release of that data does not disclose or reveal specific customer information because of the size of the group, rate classification, or nature of the information.

5.7. What Rules Reasonably Ensure the Quality and Integrity of Data and Protect its Security?

A principle of FIP is that the data collected, stored and disseminated must be reasonably accurate and complete. Another key FIP principle is that the collected data must be secure and protected from those seeking unauthorized access. To meet these two concerns, CDT recommended that the Commission adopt the following two rules:

7. DATA QUALITY AND INTEGRITY

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.

8. DATA SECURITY

(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**. Upon request by the Commission, covered entities shall notify the Commission of security breaches of covered information.

5.7.1. Position of Parties

PG&E argued that there is no need for regulation pertaining to data quality and integrity because "Commission rules and tariffs already specify the accuracy and completeness required for various types of utility information."[134]

Several other parties argued in support of the proposed Rule 8, which requires notification of the Commission concerning breaches when the Commission seeks that information.

Still other parties argued that there is no need to mandate disclosure of information breaches because notification of those affected is already required by state and federal law. PG&E contended that "[e]xisting federal and state 'red flag' laws already regulate and provide for notification of specific privacy breaches to the customers affected by the breaches."[135] CFC also argued that Civil Code § 1798.82 requires a business to "disclose any breach of the security of the system following discovery or notification of the breach in 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."[136]

PG&E and SCE argued in support of providing information on security breaches when requested by the Commission as a more practical approach than a requirement that automatically requires the provision of information.

---

[134] PG&E Reply Comments at 10.

[135] *Id*. at 10.

[136] CFC Reply Comments at 12.

5.7.2. Discussion: Modified Rules Can Promote the Quality and Security of Data

This decision rejects PG&E's recommendation to delete Rule 7, which calls for data quality and integrity. Although PG&E is correct that law and regulation already call for accurate data, since we are expanding the amount, type, and quality of consumption data that the utility will be collecting and communicating, it is appropriate to adopt this requirement.

Concerning Rule 8 on data security, it is reasonable to require utilities to notify the Commission of a breach whenever the Commission requests such a notification. However, utilities should provide an annual notification on all breaches in addition to providing such data when requested. Such information is key to the Commission's exercise of regulatory oversight and to the determination of whether additional security measures are needed. Because of this concern, automatic notifications must be provided to the Commission whenever there are significant security breaches. Utilities must therefore notify the Commission immediately when a security breach affects more that 1,000 customers. In addition, consistent with federal and state laws, covered entities must notify customers of security breaches.

In summary, this decision adopts regulation 7 as recommended by CDT for adoption by the Commission and modifies and adopts regulation 8 as follows:

> **8. DATA SECURITY**
>
> (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**. A covered third party shall notify the covered electrical corporation that is the source of the covered data

within one week of the detection of a breach. Upon a breach affecting 1,000 or more customers, whether by a covered electrical corporation or by a covered third party, the covered electrical corporation shall notify the Commission's Executive Director of security breaches of covered information within two weeks of the detection of a breach or within one week of notification by a covered third party of such a breach. Upon request by the Commission, electrical corporations shall notify the Commission's Executive Director of security breaches of covered information. In addition, electrical corporations shall file an annual report with the Commission's Executive Director, commencing with the calendar year 2012, that is due within 120 days of the end of the calendar year and notifies the Commission of all security breaches within the calendar year affecting covered information, whether by the covered electrical corporation or by a third party.

5.8. What Rules Reasonably Assure the Accountability of Entities for Complying with Privacy Policies?

Based on its analysis, CDT recommends the following rule pertaining to accountability and auditing to promote compliance with the adopted privacy policies:

9. ACCOUNTABILITY AND AUDITING

(a) **Generally**. Covered entities shall be accountable for complying with the requirements herein, and must make available to the Commission upon request or audit—

(1) the privacy notices that they provide to customers,

(2) their internal privacy and data security policies,

(3) the identities of agents, contractors and other third parties to which they disclose covered information, the purposes for which that information is disclosed, indicating for each category of disclosure whether it is for a primary purpose or a secondary purpose, and

(4) copies of any secondary-use authorization forms by which the covered party secures customer authorization for secondary uses of covered data.

(b) **Customer Complaints**. Covered entities shall provide customers with a process for reasonable access to covered information, for correction of inaccurate covered information, and for addressing customer complaints regarding covered information under these rules.

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

(d) **Audits**. Each covered entity shall conduct an independent audit of its data privacy and security practices periodically as required by the Commission to monitor compliance with its data privacy and security commitments, and shall report the findings to the Commission.

(e) **Disclosures**. On an annual basis, covered entities shall disclose to the Commission—

(1) the number of authorized third parties accessing covered information,

(2) the number of non-compliances with this rule or with contractual provisions required by this rule experienced by the covered entities or authorized third parties, and the number of customers affected by such non-compliances.

CDT argues strongly for these recommended accountability and auditing rules. CDT contends:

> Without robust and predictable accountability and auditing requirements, including regular disclosures of relevant practices to the Commission and meaningful customer redress mechanisms, there can be no oversight or enforcement, rendering the customer privacy protections fundamental to the rule ineffective. For this reason, accountability and enforcement are crucial to implementing the overall FIPs [Fair Information Practices] framework. [137]

[137] CDT Reply Comments at 8.

5.8.1. Positions of Parties

PG&E's comments expressed support for the rules as written in order to ensure that these rules avoid upending current Commission practices for addressing complaints and conducting audits.

SCE asked that the audit requirements be "triggered upon the request of the Commission"[138] and the CDT recommended rules now achieve this result.

TURN stated that:

> TURN continues to be extremely troubled by the potential lack of enforcement and lack of potential penalties to deter violations…. TURN strongly recommends the adoption of a set fine as a deterrent. We also suggest a registration process, and violations should lead to suspension, similarly to the provision for deregistering an ESP [energy service provider] under PUC Section 394.1.[139]

UCAN also highlighted enforcement in its comments, and argued that there should be a utility role in vetting third party service providers.[140] SoCalGas similarly supported a certification and registration process for third parties, but stated that it "does not believe that the IOUs represent a proper channel to provide this certification or registration function."[141] SDG&E likewise supported registration of third parties by the Commission.[142]

---

[138] SCE Reply Comments at 10.

[139] TURN Reply Comments at 9.

[140] UCAN Reply Comments at 3.

[141] SoCalGas Reply Comments at 3.

[142] SDG&E Reply Comments at 6.

5.8.2. Discussion: The Accounting and Auditing Rule Permits the Monitoring and Enforcement of Compliance with Privacy Policies

Rule 9, as recommended by CDT, offers a reasonable approach to accounting and auditing at this time. In particular, Rule 9 enables the Commission to obtain information readily so that the Commission can monitor privacy practices and exercise oversight.

At this time, there is no need to create a registration process to certify third parties to offer services in California that require access to consumption data. First, no covered entity will obtain access to an individual's consumption data without authorization from the individual, except for identified "primary purposes." Second, as a tariff condition for receiving covered information, an entity must agree to comply with the adopted privacy rules. Third, the tariff will provide that a residential customer may withdraw a third party's access to consumption data at any time and a non-residential customer will have similar rights, subject to limitation through contract consistent with the policy set forth in Rule 6(e)(2) and 6(e)(3). Fourth, the tariff will require the reporting of all security breaches by any covered entity consistent with the requirement set forth in Rule 8. Fifth, utilities and the Commission can track complaints and, if necessary, find that the third party should not be eligible to obtain consumption data from the utility because its practices fail to comply with the rules adopted. The Commission can then prohibit the provision of data services or the linkage of any device to a Smart Meter that automatically provides information to that third party and can require the removal and disconnection of all such connected devices.

In addition, it is not necessary nor is it reasonable for the Commission to regulate a customer's use of his or her own usage data. Regulating such usage

would prove both burdensome and impractical. The utilities subject to the rules adopted in this decision can provide consumers receiving usage data with information explaining the importance of protecting that data.

In summary, tariffs can protect the privacy of consumption data, empower the consumer, and provide access to the consumption data. Moreover, the approach that is adopted here does not preclude an escalation of Commission oversight should circumstances warrant. Although there is merit in the registration approach recommended by TURN, UCAN, SDG&E, and SoCalGas, this decision declines to adopt this approach because it is not necessary at this time.

The recommended rules, however, fail to provide adequate specificity concerning the filing of the required reports. For this reason, this decision adopts rules to require the privacy and security audits to take place as part of the review of a utility's operations conducted in general rate cases after 2012. In addition, the decision adopts an annual reporting requirement concerning the disclosure of information to third parties and non-compliance with contractual provisions pertaining to the privacy rules.

This decision finds reasonable and adopts the following rule:

9. ACCOUNTABILITY AND AUDITING

(a) **Generally**. Covered entities shall be accountable for complying with the requirements herein, and must make available to the Commission upon request or audit—

(1) the privacy notices that they provide to customers,

(2) their internal privacy and data security policies,

(3) the identities of agents, contractors and other third parties to which they disclose covered information, the purposes for which that information is disclosed, indicating for each

category of disclosure whether it is for a primary purpose or a secondary purpose, and

(4) copies of any secondary-use authorization forms by which the covered party secures customer authorization for secondary uses of covered data.

(b) **Customer Complaints**. Covered entities shall provide customers with a process for reasonable access to covered information, for correction of inaccurate covered information, and for addressing customer complaints regarding covered information under these rules.

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

(d) **Audits**. Each electrical corporation shall conduct an independent audit of its data privacy and security practices in conjunction with general rate case proceedings following 2012 and at other times as required by order of the Commission. The audit shall monitor compliance with data privacy and security commitments, and the electrical corporation shall report the findings to the Commission as part of the utility's general rate case filing.

(e) **Reporting Requirements**. On an annual basis, each electrical corporation shall disclose to the Commission as part of an annual report required by Rule 8.b, the following information:

(1) the number of authorized third parties accessing covered information,

(2) the number of non-compliances with this rule or with contractual provisions required by this rule experienced by the utility, and the number of customers affected by each non-compliance and a detailed description of each non-compliance.

5.9. Should We Adopt Rules Now or is Further Study Needed?

Although the Commission did not ask whether further study was needed before the adoption of privacy rules, several parties placed this issue before the Commission and the comments of many parties implicitly address the issue of timing. For this reason, this decision addresses this issue.

5.9.1. Position of Parties

SDG&E argued that "existing laws and regulations at the federal and state level, as well as numerous CPUC decisions, currently provide an adequate and proper framework to protect California citizens' energy data."[143] Nevertheless, SDG&E also proposed "to have a Commission sponsored technical working session with CDT & EFF, the IOUs and other interested parties or stakeholder to discuss the proposal and potential to 'operationalize' the adopted FIPs in more detail."[144] SDG&E proposed that the workshops develop "a set of 'use cases' to foster a better understanding of how the FIPs privacy principles may be implemented…"[145]

TURN stated that it "strongly supports the rules proposed by CDT/EFF, with some minor changes." TURN, however, also argued that "these rules still require additional details to operationalize the principles in disclosure forms, contract terms or tariff language."[146]

PG&E adopted a position similar to TURN's. PG&E stated that:

> …[It] proposes that the Commission consider adopting a new or revised General Order or policy statement on customer privacy

---

[143] SDG&E Reply Comments at 2, footnote omitted.

[144] SDG&E Reply Comments at 5.

[145] *Id.*

[146] TURN Reply Comments at 5.

> consistent with these comments. The General Order or policy statement would reaffirm and codify the Commission's existing standards and orders on customer privacy, and would also implement the customer privacy standards enacted in SB 1476.[147]

Implicit in the positions of TURN and PG&E is that the rules proposed by CDT offer a good start, but that the Commission should follow with a more general proceeding aimed at producing a new General Order on privacy.

SCE, in contrast, argued that a modified CDT proposal "would be a reasonable means of addressing customer data privacy in the context of customer interval usage data."[148]

Verizon argued that the Commission should *not* adopt privacy rules, but instead "should monitor the smart grid market for specific privacy concerns to determine whether existing privacy laws, regulations, and industry best practices adequately address such concerns or whether additional legislative or regulatory guidance is needed."[149] Implicit in this position is that the Commission can rely on SB 1476 without additional codification into regulatory rules.

5.9.2. Discussion: It is Reasonable to Adopt Rules Now

The record developed in this proceeding concerning privacy is substantial, and additional workshops to develop privacy policies, as recommended by SDG&E, are not necessary.

TURN's observation that additional details are needed to operationalize the privacy rules is well taken. The development of these details, however, can occur in the Tier 3 advice letter filings as needed. Each of PG&E, SCE and SDG&E must file a Tier 3 advice letter within 90 days of the mailing of this

[147] PG&E Opening Comments at 6.

[148] SCE Reply Comments at 2.

[149] Verizon Reply at 2.

decision that includes revisions to tariffs, where needed, to bring current practices into conformity with the privacy and security policies adopted herein.

Finally, the rules that we adopt advance the requirements and policy goals of SB 1476 and strengthen the existing statutory and regulatory frameworks that protect privacy. We therefore reject the approach recommended by some that the Commission focus on monitoring for failures to protect policy and taking remedial actions when failures occur.

6. Should Utilities Provide Price Information to Customers? What Price Information Should they Provide?

16 USC § 2621(d)(19)(B), enacted as part of national policy for the Smart Grid, contains the following requirement:

> **(B) Information**
>
> Information provided under this section, to the extent practicable, shall include:
>
> (i) Prices. Purchasers and other interested persons shall be provided with information on—
>
> (I) time-based electricity prices in the wholesale electricity market; and
>
> (II) time-based electricity retail prices or rates that are available to the purchasers.

D.09-12-046 found it unnecessary to order California utilities to provide this information because "prior Commission actions constitute a 'prior state action' and, pursuant to [16 USC] § 2622(d), no further action is required at this time,"[150] At the same time, D.09-12-046 also stated that "this decision establishes

[150] D.09-12-046 at 3.

a policy goal that SCE, PG&E, and SDG&E provide consumers with access to electricity price information by the end of 2010."[151]

Despite the clear guidance in Federal law and the Commission's own decision to establish the provision of pricing information as a policy goal, substantial issues concerning the definition of price and the usefulness of wholesale pricing information have arisen in this proceeding. This section reviews the positions of parties on this matter and decides the next steps.

6.1. Positions of Parties

Concerning the communication of pricing information, PG&E noted that it currently "provides both residential and non-residential customers with pricing information on PG&E's website, and specifically customers can obtain information about their current rate via an on-line rate information center."[152] PG&E also stated that it currently provides customers "web-based tools for forecasting and calculating their energy usage costs" and "customers can also sign up to receive email, text or phone messages as they transition from one of the upper tiers into a higher tier."[153] PG&E, however, cautioned that "the Commission should not mandate or provide prescriptive direction to utilities regarding exactly what form, or how that pricing information should be provided to customers."[154]

SCE stated that it currently provides customers with pricing data, and that "pricing data is readily available to SCE customers on SCE.com, on the

---

[151] *Id*.

[152] PG&E Reply Comments at 2.

[153] *Id*. at 3.

[154] *Id*.

customer's monthly bill, or through SCE's call center."[155] SCE also stated that it "plans to provide customers with Edison Smart Connect meters … with bill-to-date and bill-forecast information, as well as optional alerts …"[156]

Concerning pricing information in real-time or near real-time, SCE argued that "the provision of retail pricing in *near real-time* is not useful information to most customers, as tiered rate structures distort the intended affect [sic] of providing near real-time retail rates."[157] SCE claimed that this information "may cause confusion" and that "customers are far more interested in tools that help them manage their electricity bills."[158] Regarding access to pricing information in near-real time, SCE argued "the Commission should consider the value associated with performing a pilot to assess the costs and benefits…"[159] Finally, SCE argued that customers "do not face (wholesale)" prices[160] and that "there are only limited benefits from the provision of wholesale price information to customers, and any such benefits would primarily accrue to non-residential customers."[161] Based on these concerns, SCE recommended "that the Commission consider a pilot study"[162] and that "the IOUs and CAISO … work jointly in the demand response proceeding to further refine the pricing signals to develop a more effective correlation with wholesale prices."[163]

---

[155] SCE Opening Comments at A-5.

[156] *Id*.

[157] SCE Reply Comments at 13.

[158] *Id*.

[159] *Id*. at 14.

[160] *Id*. at 15.

[161] *Id*.

[162] *Id*.

[163] SCE Opening Comments at A-5 to A-6.

SDG&E stated that currently it "does not provide timely pricing data with the usage information to residential customers."[164] Concerning what pricing information it should provide, SDG&E opined "that the most useful pricing information would be an estimated price based on the expected marginal end of month bill impact given the current month-to-date (MTD) consumption and consumption patterns in past, similar periods."[165]

In sharp contrast to the position of utilities, the ISO stated that it is strongly committed to the provision of wholesale price information to customers, arguing that "[w]hile the precise wholesale price may not always convey actionable information to retail customers, providing a meaningful signal correlated with the ISO wholesale price can help customers understand when their individual action can have the greatest impact on the grid."[166] The ISO sees a rapidly evolving energy market and argued that opposition to the provision of wholesale pricing data "does not fully account for likely future developments in the area of demand response."[167]

DRA stated that it is skeptical concerning new initiatives that "require ratepayers to fund network upgrades to allow [real time] pricing signals…"[168] DRA argued that "if pricing information is to serve customers, it must be 'actionable and useful' by making clear to residential and small business customers how to save energy and money on bills."[169] Specifically, DRA

---

[164] SDG&E Opening Comments at 11.

[165] *Id*.

[166] ISO Reply Comments at 2.

[167] *Id*.

[168] DRA Reply Comments at 3.

[169] *Id*.

supported the provision of "the fully bundled rate."[170] Concerning wholesale pricing, DRA argued that "[w]holesale pricing information will not provide useful information to residential and small business customers at this time."[171]

TURN stated that it "strongly supports the comments of [DRA] and of SCE concerning the need to provide understandable and actionable data."[172] In particular, TURN supported the "provision of bill-to-date and bill forecast data"[173] and the "projected month-end tiered rate"[174] to customers. Concerning wholesale price information, TURN stated that it "appreciates the concern [that wholesale prices] … will simply confuse customers and actually promote undesirable behaviors"[175] and recommends that the Commission "redirect its focus to promote the provision of other data, at least in the near term."[176] In summary, TURN stated that it "strongly recommends that the Commission order the utilities in its next decision to implement automatic tier notification, to maximize consumer enrollment, and to report back on the statistics of enrollment."[177]

UCAN supported the provision of pricing data to customers, and argued that "[p]ricing data must incorporate the fully bundled rate per kWh rather than be limited to the commodity price."[178]

---

[170] *Id*.

[171] *Id*. at 4.

[172] TURN Reply Comments at 3.

[173] *Id*. at 4.

[174] *Id*.

[175] *Id*.

[176] *Id*.

[177] *Id*. at 5.

[178] UCAN Comments at 2.

6.2. Discussion: PG&E, SCE, and SDG&E Should Provide Retail Price Information and Make Wholesale Price Information Available

The parties have presented comments on three aspects of the issue of pricing: 1) approximations of retail prices; 2) pricing information in near real-time; and 3) wholesale prices.

On the issue of the provision of approximate price information, our record shows both substantial agreement among parties and substantial progress on the part of PG&E and SCE in making price and bill information available to customers. We find that SDG&E should join its sister utilities in making an approximate price, actual usage and an estimate of bill available to its customers a soon as possible. This information should be done in a manner consistent with PG&E and SCE in that the information should be, at a minimum, provided to customers online, available one day later, in hourly or 15 minute increments (matching the time granularity programmed into the customer's smart meter) and updated at least daily. In particular, each of the three companies should ensure that the information made available to residential and small commercial customers is updated at least on a daily basis, with each day's usage data available by the next day (the current practice), along with applicable price and cost details and with hourly or 15-minute granularity (matching the time granularity programmed into the customer's smart meter).

TURN, DRA, and UCAN provide strong support for the policy of providing "actionable" pricing data to consumers. The cautions raised by PG&E against adopting overly prescriptive disclosure requirements, particularly at this time when technology, markets, and prices are changing so rapidly, are reasonable. Nevertheless, PG&E, SCE, and SDG&E should offer to their residential customers, as TURN recommends, bill-to-date, bill forecast data,

projected month-end tiered rate, and notifications as ratepayers cross rate tiers. In addition, PG&E, SCE, and SDG&E should provide a "rate option calculator" to help customers determine whether they are on the tariff that best serves them. Furthermore, the prices conveyed should, as UCAN recommends, state the "all in" price that customers pay for electricity. It is encouraging that PG&E and SCE already provide many of these pricing data and services to their customers. At this time, pricing information does not appear to be presented in a uniform or standard manner across the utilities. As explained more fully below, PG&E, SCE, and SDG&E should provide this pricing and usage data to consumers in as near a uniform manner as possible.

Concerning wholesale prices, we endorse SCE's suggestions that we order SCE, PG&E, SDG&E, and the ISO to work together to further refine the ability to provide the wholesale price of electricity to consumers. The ISO is certainly right in its view that allowing consumers to respond to price and system conditions will require the availability of information on the status of the wholesale market. Moreover, through our workshops and the filings in this proceeding, it is clear that the ISO currently streams information continuously on its website stating several forms of the wholesale price of electricity. Thus, it should not be expensive for SCE, SDG&E, or PG&E to use this streaming information to provide information to consumers concerning a measure of prices in the wholesale market. Unfortunately, to those who are not expert in the wholesale market, the information on wholesale prices currently provided by the ISO is impenetrable. Therefore, SCE, SDG&E, and PG&E, the ISO, and consumer groups should work together to develop a cost-effective way of modifying this data to provide accessible information on prices in electric wholesale markets.

Although this decision has ordered SCE, SDG&E, and PG&E to make available bill-to-date, bill forecast data, projected month-end tiered rate, and notifications as ratepayers cross rate tiers, this decision does not prescribe how a utility should make that information available nor has it limited the information provided. As long as SCE, SDG&E, and PG&E offer to provide the information and notifications as ordered, the IOU is free to offer other information that it believes useful to its business or to advancing California energy policy.

In addition, this decision does not order SCE, SDG&E, and PG&E to use a specific technology to make the price information available. For example, a utility may wish to send the notifications of a change in rate tier via e-mail, text message, tweet, chat, or some other form of rapid communication. SCE, SDG&E, and PG&E may each propose whatever it deems a useful and cost effective way of communicating price information. The Commission's desire for the communication of pricing information, however, is not a blank check for investing in a communications backbone to establish broadband connections with meters. SCE, SDG&E, and PG&E should use as low-cost as possible means to provide pricing information, similar to the methods that they now use. SCE, SDG&E, and PG&E should make use of standardized formatting, when available, for providing this information to consumers.[179]

In summary, PG&E, SCE, and SDG&E must therefore each file a Tier 3 advice letter with the Commission within six months of the mailing of this decision that details how the utility either currently does or plans to provide

[179] The Commission is aware of many activities going on at the national level to create standardized formats around what data to provide and the means to provide customers with information through such initiatives as the OpenADE initiative. Such initiatives provide for interoperability, which is a central tenet of this Commission, the State and national and Federal Smart Grid policy-making efforts.

retail price, wholesale price, usage, and bill data to customers using the disaggregated information provided by the Smart Meter.

Finally, concerning the provision of price information in near real-time, this price information will become most useful following the deployment of HAN-enabled devices and for those customers on more dynamic tariffs, such as critical peak pricing, peak time rebate programs, and, eventually, real-time pricing. Moreover, with the complexity of current utility tariff schedules in which the rates and tiers faced by most residential customers vary by location, by day, and by amount used within the billing period, it is difficult to determine the near real-time retail price. Indeed, at several points throughout the workshops in this proceeding, it was observed that simpler tariffs would likely benefit energy customers. These considerations make us reluctant to order the provision of price information in real-time at this time, but the Commission expects to reexamine this issue in the context of the deployment of HAN and HAN-enabled devices.

In the face of this complexity and uncertainty, SCE's suggestion that the Commission encourage pilot studies on how to provide retail prices in real-time or near real-time offers a reasonable approach to this complex problem. This decision therefore orders that PG&E, SCE and SD&E each initiate a pilot study within six months to explore useful and cost-effective ways to provide price information in real-time or near real-time. PG&E, SCE, and SDG&E must consult with the Commission staff on the details of the pilot studies.

7. What Access to Usage Data Should Utilities Provide and When Should they Provide it?

This proceeding considered several ways of providing a customer with information on his or her usage discussed in this proceeding including the

provision of information over the internet with the information hosted/presented by the utility or by a third party and the provision of information through a customer premises device in direct communication with the Smart Meter, where the device is either owned by the customer or under a service contract with either the utility or a third party. In addition, it was noted that a consumer can sometimes directly install a device on his or her electric service that provides much of the information available from a Smart Meter. Finally, when a customer deploys a HAN-enabled device in their home, this device may be in communications with customer appliances or, via the internet, with other energy service entities and obtaining information simultaneously from multiple sources.

Currently, PG&E permits its customers to obtain usage data delayed by one day over the internet.[180] Similarly, SCE also permits its customers to obtain usage data delayed by one day over the internet.[181] SDG&E enables third parties, such as Google, to provide customers with information on their usage over the internet and has adopted policies to ensure that this occurs on a secure basis.[182] SDG&E's data on usage is also delayed by a day. SDG&E is planning to offer its customers access to information via a SDG&E web site in early 2011.

7.1. Position of Parties

Concerning the provision of data access, PG&E noted that "the nationwide working groups addressing both the Smart Energy 2.0 standard for HAN and the Open Automated Data Exchange (ADE) standard are addressing privacy,

[180] PG&E Opening Comments at 2.

[181] SCE Opening Comments at A-2 to A-3.

[182] SDG&E Opening Comments at 4-5.

security, and pricing models, with standards likely to be approved during 2011."[183]

SCE argued that " OpenADE efforts, now renamed 'Energy Service Provider Interface (ESPI)' have been delayed, and is [sic] now expected to be ratified by NAESB [North American Energy Standards Board] and accepted by NIST in mid-2011."[184] Despite the delay in standards adoption, SCE "plans to implement ESPI functionality using a phased approach to provide customers and authorized third parties with data access."[185]

SCE further argued:

> This phased approach will allow SCE to be best prepared to provide customers and their authorized third parties with access to usage data in timely manner once the final standard and rules are adopted by the Commission.
>
> … SCE recommends that the Commission order the IOUs to file applications in early 2011, detailing their respective plans to implement ESPI functionality, forecast costs and proposed recovery of implementation costs. Neither ESPI nor any comparable functionality was proposed in the Edison SmartConnect Application or in any other proceeding.[186]

In contrast to SCE and PG&E, SDG&E already provides access to third parties. In particular, "SDG&E provided residential customers with Smart Meters the option to access their hourly interval consumption data via Google's PowerMeter."[187] SDG&E's Reply Comments provided details on the procedures that customers must follow to give an authorized third-party access to usage

---

[183] PG&E Reply Comments at 4.

[184] SCE Reply Comments at 11-12.

[185] *Id.* at 12.

[186] *Id*.

[187] SDG&E Opening Comments at 12.

data as well as the numerous security steps that SDG&E and Google have implemented to protect customer data from those attempting to secure access fraudulently.

TURN also provided extensive comments concerning issues that arise from providing customers and authorized third parties access to usage data. In particular, TURN argued that there is a difference between third parties who obtain usage information from an internet connection with the utility (referred to as the backhaul) and those that receive information from a device bolted to the customer's line or directly from the customer's meter. TURN stated:

> The backhaul data is collected without any customer input, and the data is available only because the utilities installed the new communicating interval meters on the premises of residential and small commercial customers. These customers had no choice in the collection of the consumption data. For this reason, any dissemination of backhaul data should be highly protected through the rules proposed by CDT/EFF.[188]

At the other end of the spectrum, TURN noted that

> … a customer can choose to voluntarily install "bolt-on technologies" to their meter and obtain real-time meter wireless output signal data to their own HAN Systems…[t]he customer chooses to obtain this data irrespective of any action by the utility, and should thus have complete control over the disposition of the data.[189]

In contrast to data access through the backhaul and data access through a measurement device attached near the meter, TURN argued that data from the smart meter obtained through communication with the meter falls between these two poles and requires a different approach. TURN urged that the Commission

[188] TURN Reply Comments at 11-12.

[189] *Id*. at 12.

"should require that utilities file a Tier 3 advice letter prior to any authorization/registration of devices to read the meter signal" and proposes requirements governing this process.[190]

EnerNOC argued for providing customers and their agents with full access to usage data generated by the Smart Meter as soon as possible:

> EnerNOC believes that customers, and their authorized agents, should have access to data on a real-time basis at the meter through Zigbee[191]-enabled devices using Smart Energy Profile (SEP) protocol[192] as soon as possible. Customers, or their agents, should be able to access all data recorded by the meter on as granular a basis as is possible. While not all customers may want or need this capability, the smart meters should be able to provide a choice of data interval and SEP is available today (version 1.0).[193]

Control4 similarly urged that the Commission should order consumer access to their Smart Meter data quickly and directly. Control4 argued that the Commission should order the use of communication standard SEP 1.0 rather than waiting for SEP 2.0.[194] "The individual consumption data communicated in near real time (i.e., every ten seconds) via SEP 1.0 is more than adequate to provide consumers with analytics about their usage patterns, contextualized energy efficiency tips, and energy costs.[195]

---

[190] *Id*. at 13-14.

[191] Zigbee is a specification for a suite of high level communication protocols using small, low-power digital radios for low-data-rate wireless personal area networks.

[192] Smart Energy Profile (SEP) is a particular protocol in the Zigbee series. SEP 1.0 is currently available and SEP 2.0 is under development.

[193] EnerNOC Opening Comments at 10-11.

[194] SEP 2.0 is anticipated to provide better security features, among other features, than is available in SEP 1.0.

[195] Control4 Reply Comments at 2.

Tendril argued that access to meter information should be provided immediately by SDG&E, PG&E, and SCE. Tendril stated that it fails "to see any justification in the record of this proceeding to support the assertion by SCE that achieving the objective established by the Commission is in any way 'dependent' on the development of a future standard."[196]

7.2. Discussion

TURN is right to suggest that Smart Meter data provided by PG&E, SCE, or SDG&E via the internet (or the backhaul) should be subject to protections because consumers do not need to take any affirmative action to either acquire the data or to make it available to others. The measures adopted in this decision protect that data and require an affirmative action by the customer before making the data available for secondary purposes.

There is no reason why SCE and PG&E should not provide access to authorized third parties to consumer usage data available through the backhaul as SDG&E already does. SCE and PG&E are right to point out that full OpenADE or ESPI standards are not yet adopted, but the lack of final standards has not stopped SDG&E from making available data that has enabled Google to provide consumption information to participating SDG&E customers.

The necessity of an application, as SCE requests, to consider the recovery of costs for third-party access is not clear. SDG&E gained Commission authorization for providing information to third parties through a Tier 2 advice letter that was only three pages in length (plus tariff sheets). Moreover, concerning implementation costs, SDG&E's advice letter states, "[i]mplementation costs are estimated between $650K and $750K, funded

[196] Tendril Opening Comments at 9, footnote omitted.

through current AMI contingency funding and energy efficiency education and outreach funding."[197] Subsequently, the Commission approved SDG&E's tariff that made the Google service possible through a one sentence administrative letter.

Therefore, PG&E and SCE shall each file a Tier 3 advice letter with corresponding tariffs to provide third-parties, when authorized by the consumer and when agreeing to the privacy protections adopted in this decision, access to the usage data. This filing is due within six months of the mailing of this decision. Furthermore, SDG&E should file an advice letter within six months of the mailing of this decision that modifies its current tariff to bring its tariff into conformity with the rules adopted in this decision.

Ordering third-party access to usage data is reasonable and in the public interest. California ratepayers have incurred substantial costs to modernize the electric meters throughout the state. Many of the benefits of these new meters will not be realized until customers can obtain access to their usage data through utilities or through third parties, like Google, who specialize in the presentment of actionable information to consumers. We see no reason to delay this further.

Providing direct access to the granular data through connecting a device to the Smart Meter, however, raises similar issues concerning privacy, but different technical issues. In particular, we see little difference between those third parties that obtain access with customer assent to information via the internet and those third parties that obtain access through the HAN with a device that is "locked" and automatically transmits meter data to that one party. This decision finds that the granular nature of the data collected at the Smart Meter requires the same privacy protections as those protections adopted for the less granular data

[197] SDG&E, Advice Letter 2100-E (July 31, 2009) at 2.

that can be distributed by PG&E and SCE and is currently provided to Google by SDG&E over the internet.

As this proceeding developed, adoption of SEP 2.0 standard was anticipated. With the continuing delays in the development of SEP 2.0, it is reasonable to order SCE, SDG&E, and PG&E to work with Commission staff to develop and implement pilot projects within six months that connect HAN-enabled devices to Smart Meters. The goal of these pilots is to determine the best and most timely way of providing California customers with secure, private, and direct access to the disaggregated data available in the Smart Meters. To the extent practical, PG&E, SCE, and SDG&E should collaborate in order to ensure that the pilot studies work towards providing a common interface for the devices of customers and third parties.

These pilot studies should include a sufficient number of customers as to make the results statistically meaningful. The purposes of these pilot studies are to determine the availability of HAN-enabled devices, the robustness of the utilities' HAN, and should provide for a strategy to implement full activation of the HAN across the service territory as soon as is feasible.. This pilot should also be used to begin the testing and certification of devices that can be made available to customers participating in this pilot, and beyond.

8. Conclusion

This decision, based on an extensive record discussed above, has adopted rules and procedures to protect the privacy and security of consumer usage information and ordered PG&E, SCE, and SDG&E to bring their practices into conformity with the rules adopted here and contained in Attachment D. These rules implement policies contained in the Pub. Util. Code and those adopted in SB 1476. Each utility must file a Tier 3 advice letter within 90 days of the mailing

of this decision that includes revisions to tariffs, where needed, to bring current practices into conformity with the privacy and security policies adopted herein.

The decision requires PG&E, SCE, and SDG&E to file within six months an advice letter that provides price, usage and costs information to customers. The decision specifies that PG&E, SCE, and SDG&E provide residential customers certain useful data, including bill-to-date, forecast of bills, projected month-end tiered rate, a rate calculator, and offer notifications as residential customers cross rate tiers..

The decision also orders PG&E and SCE, to file within six months an advice letter that provides third parties access to consumer usage data consistent with the privacy and security provisions adopted in Attachment D. SDG&E, which currently provides such access, should file any tariff revisions needed to ensure that its current program conforms with the provisions of Attachment D, if such revisions are needed. This tariff filing is due within six months of the mailing of this decision.

The decision also orders PG&E, SCE, and SDG&E to commence within six months a pilot study to provide retail price information in real-time or near-real-time. In addition, PG&E, SCE, and SDG7E shall also commence within six months a pilot study that provides direct access to the information in the Smart Meter and supports for HAN-enabled devices.

These policies will provide customers with access to the services and features supported by Smart Meters and will help California ratepayers to realize more of the benefits afforded by Smart Meters.

Finally, the Commission initiates a new phase of this proceeding to determine whether the rules and policies adopted in this decision should apply

to gas corporations, community choice aggregators, electric service providers and electrical corporations other than PG&E, SCE, and SDG&E..

9. Comments on Proposed Decision

The proposed decision of President Peevey in this matter was mailed to the parties in accordance with Section 311 of the Public Utilities Code and comments were allowed under Rule 14.3 of the Commission's Rules of Practice and Procedure. Comments were filed on _____, and reply comments were filed on _____ by _____.

10. Assignment of Proceeding

President Michael R. Peevey is the assigned Commissioner and Timothy J. Sullivan is the assigned Administrative Law Judge in this proceeding.

Findings of Fact

1. The Department of Homeland Security developed a framework for information systems affecting national security called Fair Information Practice (FIP) principles. The framework includes eight principles: (1) Transparency, (2) Individual Participation, (3) Purpose Specification, (4) Data Minimization, (5) Use Limitation, (6) Data Quality and Integrity, (7) Security, and (8) Accountability and Auditing.

2. The FIP principles are consistent with emerging national privacy and security principles recommended by the Department of Homeland Security.

3. The FIP principles offer a practical tool for developing rules to protect the privacy and security of electricity usage data.

4. The principle of data minimization will promote the security of data.

5. Data quality and integrity is critical to the rendering of accurate and reasonable bills.

6. It is reasonable to require PG&E, SCE, and SDG&E to adopt policies applying to themselves and those with whom they contract in the provision of operational services that comply with SB 1476 and the privacy rules adopted in this decision.

7. It is reasonable to exempt from the privacy and security requirements in this decision third parties obtaining information on the usage of ten or less households because failure to do so would complicate situations where a family member or friend takes care of the affairs of a small number of other people.

8. It is reasonable to exempt consumers from privacy and security requirements in this decision that apply to third parties obtaining usage data. Consumers may use their usage data as they wish.

9. It is reasonable to require third parties who receive consumer usage information from the electric corporation via the internet ("back-haul") or from the Smart Meter through a "locked" HAN-enabled device that transmits usage data to the third party to comply with the privacy and security requirements adopted in this decision.

10. It is reasonable to define a customer, for the purposes of these rules, as any entity receiving retail generation, distribution or transmission service from an investor-owned electric utility.

11. It is reasonable to open another phase of this proceeding to determine whether the rules and policies adopted in this decision should also apply to gas corporations, community choice aggregators, electric service providers and electric corporations other than PG&E, SCE, and SDG&E.

12. It is reasonable to define as "covered information" any electrical usage information obtained through the use of the capabilities of Advanced Metering Infrastructure when associated with any information that can reasonably be used

to identify a customer, except that covered information does not include usage information from which identifying information has been removed such that a customer cannot reasonably be identified or re-identified.

13. It is reasonable to adopt different rules depending on the purpose for the collection of the usage information.

14. It is reasonable to define as "primary purposes" information that is used to:

(1) provide or bill for electrical power,

(2) fulfill other operational needs of the electrical system or grid,

(3) provide services as required by state or federal law or specifically authorized by an 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.

15. It is reasonable to define as a "secondary purpose" any purpose that is not a primary purpose.

16. Electronic transactions are growing in importance throughout the economy.

17. It is reasonable to require covered entities to provide information on their privacy policy when confirming a new customer account or new customer relationship.

18. It is not reasonable to require that a covered entity use a title for the name of the privacy document that is specified by regulation.

19. It is reasonable to require that privacy policies be written so that the policies are "reasonably understandable."

20. It is reasonable for a covered entity to provide customers with access to prior versions of privacy policies in the event that a customer desires such access.

21. It is reasonable to require covered entities to ensure the transparency of their privacy policies by providing customers with notice that meet the following requirements:

2. TRANSPARENCY (NOTICE)

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

(b) **When Provided**. Covered entities shall provide written or electronic notice when confirming a new customer account and at least twice a year informing customers how they may obtain a copy of the covered entity's privacy policy regarding the collection, storage, use, and disclosure of covered information, and shall provide conspicuous posting of the notice and privacy policy or link to the notice and privacy policy on the home page of their website, and shall include a link to their notice and privacy policy in all electronic correspondence to customers.

(c) **Form**. The notice shall be labeled to make clear that it is a privacy notice and the notice shall communicate where a consumer may find policies affecting the collection, storage, use and disclosure of energy usage information and shall—

(1) be written in easily understandable language, and

(2) be no longer than is necessary to convey the requisite information.

(d) **Content.** The notice and the posted privacy policy shall state clearly—

(1) the identity of the covered entity,

(2) the effective date of the notice or posted privacy policy,

(3) the covered entity's process for altering the notice or posted privacy policy, including how the customer will be informed of any alterations, and where prior versions will be made available to customers, and

(4) the title and contact information, including email address, postal address, and telephone number, of an official at the covered entity who can assist the customer with privacy

> questions, concerns, or complaints regarding the collection, storage, use, or distribution of covered information.

22. Because of the large and changing number of companies that receive access to information concerning consumers when assisting the utility in its operations, because the Commission can obtain the identities of all companies receiving information for a utility, and because the Commission requires utilities to ensure that companies supporting utilities in utility operations follow the same rules as the utility, it is unreasonable to require the disclosure of the identities of all companies receiving information from the utility.

23. Providing consumers with information on the categories of customers receiving information from a covered entity provides sufficient information to customers to enable them to understand the potential uses of their information.

24. It is reasonable to require utilities to ensure that companies supporting utilities in utility operations follow the same rules as the utility and to ensure that they cannot use information pertaining to a customer for any purpose other than the purpose for which the utility had contracted their services.

25. It is reasonable to adopt further rules pertaining to disclosure of the specific purposes for which the information is collected as follows:

> **3. PURPOSE SPECIFICATION**
>
> The notice required under section 2 shall provide—
>
> (a) an explicit description of—
>
> (1) each category of covered information collected, used, stored or disclosed by the covered entity, and, for each category of covered information, the reasonably specific purposes for which it will be collected, stored, used, or disclosed, and
>
> (2) each category of covered information that is disclosed to third parties, and, for each such category, (i) the purposes for

which it is disclosed, and (ii) the number and categories of third parties to which it is disclosed;

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

(c) a description of—

(1) the means by which customers may view, inquire about, or dispute their covered information, and

(2) the means, if any, by which customers may limit the collection, use, storage or disclosure of covered information and the consequences to customers if they exercise such limits.

26. It is not reasonable to require the advance notice of a request by an authority for access to data held by a covered entity in all circumstances.

27. It is reasonable to require a report from covered entities on disclosures of covered information made pursuant to legal process when the Commission requests the preparation of such a report.

28. The following rules which provide individuals with access and control of their covered information are reasonable and promote the Fair Information Practice principle of individual participation.

4. INDIVIDUAL PARTICIPATION (ACCESS AND CONTROL)

(a) **Access**. Covered entities shall provide to customers upon request convenient and secure access to their covered information in an easily readable format that is at a level no less detailed than that at which the covered entity discloses the data to third parties.

(b) **Control**. Covered entities shall provide customers with convenient mechanisms for—

(1) granting and revoking authorization for secondary uses of covered information,

(2) disputing the accuracy or completeness of covered information that the covered entity is storing or distributing for any primary or secondary purpose, and

(3) requesting corrections or amendments to covered information that the covered entity is collecting, storing, using, or distributing for any primary or secondary purpose.

(c) **Disclosure Pursuant to Legal Process**.

(1) Except as otherwise provided in this rule or expressly authorized by state or federal law or by order of the Commission, a covered entity shall not disclose covered information except pursuant to a warrant or other court order naming with specificity the customers whose information is sought. Unless otherwise directed by a court, law, or order of the Commission, covered entities shall treat requests for real-time access to covered information as wiretaps, requiring approval under the federal or state wiretap law as necessary.

(2) Unless otherwise prohibited by court order, law, or order of the Commission, a covered entity, upon receipt of a subpoena for disclosure of covered information pursuant to legal process, shall, prior to complying, notify the customer in writing and allow the customer 7 days to appear and contest the claim of the person or entity seeking disclosure.

(3) Nothing in this rule prevents a person or entity seeking covered information from demanding such information from the customer under any applicable legal procedure or authority.

(4) Nothing in this section prohibits a covered entity from disclosing covered information with the consent of the customer, where the consent is express, in written or electronic form, and specific to the purpose and to the person or entity seeking the information.

(5) Nothing in this rule prevents a covered entity from disclosing, in response to a subpoena, the name, address and other contact information regarding a customer.

(6) Upon request of the Commission, covered entities shall report to the Commission on disclosures of covered information made pursuant to legal process. The Commission may make such reports publicly available without identifying the affected customers, unless making

such reports public is prohibited by state or federal law or by order of the Commission.

(d) **Disclosure of Information in Situations of Imminent Threat to Life or Property.** These rules concerning access, control and disclosure do not apply to information provided to emergency responders in situations involving an imminent threat to life or property.

29. Data minimization promotes privacy and security by limiting the amount of personal data collected and the amount that must be secured and protected.

30. It is reasonable to minimize the amount of personal data collected in order to promote the privacy and security of data.

31. Adopting a principle of data minimization will be a new approach in the regulation of electric utilities.

32. The data historically collected by electric utilities and the Commission most commonly concerned costs of providing electric service, the demand for electric service, billing data and company revenues.

33. A principle of data minimization can serve as a guide for the revision and development of other regulations pertaining to the collection and retention of information.

34. There is a tension between a principle of data minimization and the Commission's need for data to exercise effective oversight of utility operations and programs.

35. It is appropriate to permit the collection of data that is reasonably necessary and for as long as is reasonably necessary.

36. The Commission creates data collection and retention requirements as part of its regulatory program. These requirements carry Commission authorization for the collection and retention of data.

37. It is reasonable to set a time period for the retention of data that is not open-ended.

38. Data minimization is a "best practice" in a strategy to protect and secure the usage data of electric utility customers.

39. It is reasonable to adopt the following rules that apply to covered entities to encourage the protection of the privacy and security of usage data through a strategy of data minimization.

> **5. DATA MINIMIZATION**
>
> (a) **Generally**. Covered entities shall collect, store, use, and disclose only as much covered information as is reasonably necessary or as authorized by the Commission to accomplish a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.
>
> (b) **Data Retention**. Covered entities shall maintain covered information only for as long as reasonably necessary or as authorized by the Commission to accomplish a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.
>
> (c) **Data Disclosure**. Covered entities shall not disclose to any third party more covered information than is reasonably necessary or as authorized by the Commission to carry out on behalf of the covered entity a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

40. It is reasonable for an electrical corporation to collect, store and use covered information for primary purposes, as defined above, on the condition that they follow the restrictions found reasonable in Finding of Fact 51.

41. It is reasonable to permit other covered entities to collect, store and use covered information when they have the prior consent of a customer, on the condition that they follow the restrictions found reasonable in Finding of Fact 51.

42. It is reasonable to require covered entities to ensure compliance of contractors with the privacy and security policies adopted herein through the "chain of responsibility" concept, whereby the responsible entity terminates business with contracts who fail to follow the privacy and security policies adopted in this decision.

43. It is reasonable that tariffs that make customer usage information available to authorized third parties contain a provision that enables a residential customer to withdraw authorization at any time.

44. It is not in the public interest for a customer's authorization of the disclosure of information to a third party to automatically expire after two years.

45. It is reasonable to require a covered entity receiving usage information for a non-primary purpose to provide a residential customer with an annual reminder of the prior authorization and an opportunity to opt out.

46. It is reasonable to modify the disclosure rules in order to ensure that the rules do not upset contractual arrangements between non-residential customers and third parties.

47. It is reasonable to permit non-residential customers to authorize the disclosure to a third party of usage data pursuant to the terms of any commercial contract of finite duration.

48. It is not reasonable to prohibit customers from authorizing the disclosure of usage data for secondary purposes because to do so would unreasonably abridge a customer's control of his usage data.

49. Determining which activities should be "eligible" secondary purposes would be burdensome.

50. Requiring regulatory reviews to determine which secondary purposes would be "eligible" to obtain usage data from customers (when authorized) could have a chilling effect on product and service innovation in California.

51. It is reasonable to adopt the following rules that apply to covered entities to limit the use and disclosure of consumer usage information:

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 electrical corporation may collect, store and use covered information for primary purposes without customer consent. Other covered entities may collect, store and use covered information only with prior customer consent, except as otherwise provided here.

(c) **Disclosures to Third Parties**.

(1) **Initial Disclosure by a Covered Entity**. A covered entity may disclose covered information to a third party without customer consent when explicitly ordered to do so by the Commission or 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 consistent with applicable program terms and conditions, unless otherwise directed by the Commission.

(2) **Subsequent Disclosures**. Any entity that receives covered information derived initially from a covered entity may disclose such covered information to another entity without

customer consent for a primary purpose, provided that the entity disclosing the covered information shall, by contract, require the entity receiving the covered information to use the covered information only for such primary purpose and to agree to store, use, and disclose the covered information under policies, practices and notification requirements no less protective than those under which the covered entity from which the covered information was initially derived operates as required by this rule.

(3) **Terminating Disclosures to Entities Failing to Comply With Their Privacy Assurances**. When a covered entity discloses covered information to a third party under this subsection 6(c), it shall specify by contract that it shall be considered a material breach if the third party engages in a pattern or practice of storing, using or disclosing the covered information in violation of the third party's contractual obligations to handle the covered information under policies no less protective than those under which the covered entity from which the covered information was initially derived operates in compliance with this rule. If a covered entity disclosing covered information finds that a third party to which it disclosed covered information is engaged in a pattern or practice of storing, using or disclosing covered information in violation of the third party's contractual obligations related to handling covered information, the disclosing entity shall promptly cease disclosing covered information to such third party.

(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. This authorization is not required when information is—

(1) provided pursuant to a legal process as described in 4(c) above;

(2) provided in situations of imminent threat to life or property as described in 4(d) above; or

(3) authorized by the Commission pursuant to its jurisdiction and control.

(e) **Customer Authorization**.

(1) **Authorization**. Separate authorization by each customer must be obtained for each secondary purpose.

(2) **Revocation**. Customers have the right to revoke, at any time, any previously granted authorization. Non-residential customers shall have the same right to revoke, unless specified otherwise in a contract of finite duration.

(3) **Opportunity to Revoke**. The consent of a residential customer shall continue without expiration, but an entity receiving information pursuant to a residential customer's authorization shall contact the customer, at least annually, to inform the customer of the authorization granted and to provide an opportunity for revocation. The consent of a non-residential customer shall continue in the same way, unless specified otherwise in a contract of finite duration, but an entity receiving information pursuant to a non-residential customer's authorization shall contact the customer, to inform the customer of the authorization granted and to provide an opportunity for revocation either upon the termination of the contract, or annually if there is no contract..

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

(g) **Availability of Aggregated Usage Data**. Covered entities shall permit the use of aggregated usage data that is removed of all personally-identifiable information to be used for analysis, reporting or program management provided that the release of that data does not disclose or reveal specific customer information because of the size of the group, rate classification, or nature of the information.

52. Because the usage data collected by smart meters expands the type and amount of information, it is reasonable to adopt rules to require data quality and integrity.

53. Because covered entities must notify customers of security breaches, there is no need for the covered entities to notify the Commission each time a security breach occurs.

54. Because of the Commission's responsibility to exercise regulatory oversight concerning the security of usage data, it is reasonable to require all covered electrical corporations to provide the Commission with a report on security breaches annually or upon a breach affecting more than 1,000 customers.

55. It is reasonable to adopt the following rules to protect data quality and integrity and to provide for data security:

> **7. DATA QUALITY AND INTEGRITY**
>
> 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.
>
> **8. DATA SECURITY**
>
> (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**. A covered third party shall notify the covered electrical corporation that is the source of the covered data within one week of the detection of a breach. Upon a breach affecting 1,000 or more customers, whether by a covered electrical corporation or by a covered third party, the covered electrical corporation shall notify the Commission's Executive Director of security breaches of covered information within two weeks of the detection of a breach or within one week of notification by a covered third party of such a breach. Upon request by the Commission, electrical corporations shall notify the Commission's Executive Director of security breaches of covered information. In addition, electrical corporations shall file an annual report with the Commission's Executive Director, commencing with the calendar year 2012, that is due within 120 days of the end of the calendar year

and notifies the Commission of all security breaches within the calendar year affecting covered information, whether by the covered electrical corporation or by a third party.

56. Under the rules adopted in this decision, no covered entity will obtain access to an individual's consumption data without authorization from the individual except for that information used to meet a primary purpose, as defined in this decision.

57. As a tariff condition for obtaining access to usage data for a non-primary purpose, an entity must agree to comply with the adopted privacy rules.

58. Because of the privacy protections adopted in this decision, because a residential customer may withdraw access to his or her consumption data at any time, and because the Commission can find a third party ineligible to receive data either via tariff or by refusing to interconnect a device that automatically transfers usage data to the third party, it is not necessary to create a registration process to certify third parties as eligible to receive usage data.

59. It is not necessary for the Commission to regulate a customer's use of his or her own usage data.

60. It would burdensome and impractical to regulate a customer's use of his or her own usage data.

61. Electric utilities can provide consumers receiving usage data either over the internet (the back haul) or through the Smart Meter with information explaining the importance of protecting that data.

62. The following rules to promote the accountability of covered entities for compliance with the requirements adopted in this decision and to permit the auditing of compliance are reasonable:

9. ACCOUNTABILITY AND AUDITING

(a) **Generally**. Covered entities shall be accountable for complying with the requirements herein, and must make available to the Commission upon request or audit—

(1) the privacy notices that they provide to customers,

(2) their internal privacy and data security policies,

(3) the identities of agents, contractors and other third parties to which they disclose covered information, the purposes for which that information is disclosed, indicating for each category of disclosure whether it is for a primary purpose or a secondary purpose, and

(4) copies of any secondary-use authorization forms by which the covered party secures customer authorization for secondary uses of covered data.

(b) **Customer Complaints**. Covered entities shall provide customers with a process for reasonable access to covered information, for correction of inaccurate covered information, and for addressing customer complaints regarding covered information under these rules.

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

(d) **Audits**. Each electrical corporation shall conduct an independent audit of its data privacy and security practices in conjunction with general rate case proceedings following 2012 and at other times as required by order of the Commission. The audit shall monitor compliance with data privacy and security commitments, and the electrical corporation shall report the findings to the Commission as part of the utility's general rate case filing.

(e) **Reporting Requirements**. On an annual basis, each electrical corporation shall disclose to the Commission as part of an annual report required by Rule 8.b, the following information:

(1) the number of authorized third parties accessing covered information,

(2) the number of non-compliances with this rule or with contractual provisions required by this rule experienced by the utility, and the number of customers affected by each non-compliance and a detailed description of each non-compliance.

63. The record in this proceeding concerning privacy is substantial.

64. Additional workshops to develop privacy policies at this time are not necessary.

65. Tier 3 advice letter filings, comments and Commission review can lead to adoption of the detailed procedures and forms needed to operationalize the privacy rules adopted in this decision.

66. PG&E and SCE have made substantial progress in making price information available to consumers over the internet.

67. It is reasonable to require PG&E, SCE, and SDG&E to provide approximate price information to customers.

68. PG&E, SCE, and SDG&E should provide actionable pricing data to consumers.

69. It is reasonable to require that PG&E, SCE, and SDG&E offer to customers – at a minimum – bill-to-date, bill forecast, projected month-end tiered rate, a rate calculator, and notifications to ratepayers, if desired, when the customers cross rate tiers.

70. It is reasonable for PG&E, SCE, and SDG&E to provide customers with an "all in" price that the customers pay for electricity.

71. It is reasonable to require PG&E, SCE, and SDG&E each to file a Tier 3 advice letter within 90 days of the mailing of this decision to bring policies, practices and tariffs into conformity with the rules adopted in Attachment D.

72. It is reasonable to require PG&E, SCE, and SDG&E each to file a Tier 3 advice letter within six months of the mailing of this decision to provide pricing, usage and cost data, as specified herein, to customers via an online service offered by the utility.

73. The provision of price information in real-time or near real-time will be most useful following the deployment of HAN-enabled devices.

74. The provision of price information in real-time or near real-time will be most useful to consumers if the Commission adopts real-time-prices or critical peak pricing tariffs.

75. The complexity of current tariff schedules makes it difficult to determine the real-time or near real-time price charged for electricity.

76. Since the HAN is not yet activated, it is not reasonable to order the provision of price information in real-time or near real-time at this time.

77. SDG&E has provided a customer's usage data to Google for presentation to the consumer when the consumer has authorized this action.

78. It is reasonable to require SCE and PG&E to provide access to a consumer's usage data to an authorized third party at this time.

79. SDG&E obtained Commission approval to provide a customer's usage data to an authorized third party via a Tier 3 advice letter.

80. It is reasonable to order third-party access to usage data when authorized by the customer.

81. It is reasonable to require PG&E, SCE, and SDG&E to file a Tier 3 advice letter within six months of the mailing of this decision to provide third-party access to usage data consistent with the privacy rules adopted in this decision. It is reasonable to require that the advice letters of PG&E and SCE propose a process to offer third-parties access to customer usage data, when authorized, in

a matter consistent with the privacy and security policies contained in Attachment D. It is reasonable to require the advice letter of SDG&E to show that the third-party access to customer usage data that it now provides is done in a manner consistent with the privacy and security policies adopted in Attachment D.

82. It is reasonable to require that PG&E, SCE, and SDG&E each commence a pilot study that offers price information to customers in real-time or near-real-time.

83. The usage data provided by a Smart Meter to a HAN-enabled device is very granular and can provide information that discloses a household's use of appliances and daily habits.

84. Many of the benefits of a Smart Meter arise from establishing a home area network that has access to the granular data produced by the Smart Meters.

85. It is reasonable to order SCE, SDG&E, and PG&E to commence pilot studies within six months of the mailing of this decision that permits HAN-enabled devices to be connected directly with the Smart Meters.

86. It is reasonable to require PG&E, SCE, and SDG&E to coordinate with the California ISO to determine an effective and inexpensive way to make wholesale pricing data available to those California customers who desire this information.

Conclusions of Law

1. SB 1476 (Chapter 497, Statutes of 2010) clarified Commission responsibility and authority to protect the privacy and security of customer usage data arising from Smart Meters.

2. The FIP principles of Transparency, Individual Participation, Purpose Specification, Use Limitation and Data Security can be linked to the provisions of SB 1468 and the Pub. Util. Code as detailed herein.

3. The FIP principles are consistent with SB 1476 and other California statutes.

4. Using the FIP principles as guides for developing California policies and regulations that aim to protect the privacy and security of customer data is reasonable.

5. SB 1476 provides guidance and authority to the Commission to protect the privacy of energy consumption data in the possession of utilities or in the possession of third parties responsible for system, grid, or operational needs, or energy efficiency programs.

6. Tariffs can require compliance with privacy and security provisions as a condition for permitting a HAN-enabled device to communicate directly with a Smart Meter.

7. In situations where a HAN-enabled device is "locked" to a third party and automatically forwards customer usage data to that third party and no other, it is consistent with California law and policy to require a condition for access to the Smart Meter that the customer agrees to the data transfer and to the third party's proposed uses of the data and that the third party demonstrate compliance with Commission requirements for protecting customer data and customer privacy.

8. Requiring that third parties protect customer data and privacy as conditions of the tariff that offers third parties, with customer approval, access to customer usage data is consistent with the intent and language of SB 1476.

9. Requiring privacy and security protections by third parties acquiring consumption data from a Smart Meter assures equal treatment with those that acquire usage data over the internet from the utility.

10. The use of tariffs to regulate the connection of devices to the Smart Meter is consistent with Commission regulatory practice.

11. The Order Instituting Rulemaking that initiated this proceeding set the general scope of this proceeding as that of considering further actions pertaining to electric utilities and the smart grid. It did *not* include gas companies, community choice aggregators, or electric service providers.

12. SB 1476 applies to the customer usage data of electric and gas corporations.

13. Holding covered entities responsible for meeting the following requirements to ensure the transparency of privacy notices and policy is consistent with SB 1476, relevant provisions of the Pub. Util. Code and past Commission policies to protect privacy:

> **2. TRANSPARENCY (NOTICE)**
>
> (a) **Generally**. Covered entities shall provide customers with meaningful, clear, accurate, specific, and comprehensive notice regarding the collection, storage, use, and disclosure of covered information.
>
> (b) **When Provided**. Covered entities shall provide written or electronic notice when confirming a new customer account and at least twice a year informing customers how they may obtain a copy of the covered entity's privacy policy regarding the collection, storage, use, and disclosure of covered information, and shall provide conspicuous posting of the notice and privacy policy or link to the notice and privacy policy on the home page of their website, and shall include a link to their notice and privacy policy in all electronic correspondence to customers.
>
> (c) **Form**. The notice shall be labeled to make clear that it is a privacy notice and the notice shall communicate where a consumer may find policies affecting the collection, storage, use and disclosure of energy usage information and shall—
>
> (1) be written in easily understandable language, and
>
> (2) be no longer than is necessary to convey the requisite information.

(d) **Content.** The notice and the posted privacy policy shall state clearly—

(1) the identity of the covered entity,

(2) the effective date of the notice or posted privacy policy,

(3) the covered entity's process for altering the notice or posted privacy policy, including how the customer will be informed of any alterations, and where prior versions will be made available to customers, and

(4) the title and contact information, including email address, postal address, and telephone number, of an official at the covered entity who can assist the customer with privacy questions, concerns, or complaints regarding the collection, storage, use, or distribution of covered information.

14. The Commission may obtain access to the names of companies receiving data from a utility regulated by the Commission.

15. A utility may impose privacy restrictions on firms with which it contracts.

16. Holding covered entities responsible for meeting the following requirements pertaining to the disclosure of the purposes for which information is collected, used, stored or disclosed is consistent with SB 1476, relevant provisions of the Pub. Util. Code and past Commission policies to protect privacy:

3. PURPOSE SPECIFICATION

The notice required under section 2 shall provide—

(a) an explicit description of—

(1) each category of covered information collected, used, stored or disclosed by the covered entity, and, for each category of covered information, the reasonably specific purposes for which it will be collected, stored, used, or disclosed, and

(2) each category of covered information that is disclosed to third parties, and, for each such category, (i) the purposes for

which it is disclosed, and (ii) the number and categories of third parties to which it is disclosed;

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

(c) a description of—

(1) the means by which customers may view, inquire about, or dispute their covered information, and

(2) the means, if any, by which customers may limit the collection, use, storage or disclosure of covered information and the consequences to customers if they exercise such limits.

17. Rules that provide the individual customer with access to and control over his or her own usage information promote individual participation in the information collection and are consistent with the FIPs and California law.

18. It is not necessary to require the advance notice of a request by an authority for access to data held by a covered entity in all circumstances.

19. The following rules to provide individuals with access and control of their covered information are consistent with SB 1476 and California law and policies:

4. INDIVIDUAL PARTICIPATION (ACCESS AND CONTROL)

(a) **Access**. Covered entities shall provide to customers upon request convenient and secure access to their covered information in an easily readable format that is at a level no less detailed than that at which the covered entity discloses the data to third parties.

(b) **Control**. Covered entities shall provide customers with convenient mechanisms for—

(1) granting and revoking authorization for secondary uses of covered information,

(2) disputing the accuracy or completeness of covered information that the covered entity is storing or distributing for any primary or secondary purpose, and

(3) requesting corrections or amendments to covered information that the covered entity is collecting, storing, using, or distributing for any primary or secondary purpose.

(c) **Disclosure Pursuant to Legal Process**.

(1) Except as otherwise provided in this rule or expressly authorized by state or federal law or by order of the Commission, a covered entity shall not disclose covered information except pursuant to a warrant or other court order naming with specificity the customers whose information is sought. Unless otherwise directed by a court, law, or order of the Commission, covered entities shall treat requests for real-time access to covered information as wiretaps, requiring approval under the federal or state wiretap law as necessary.

(2) Unless otherwise prohibited by court order, law, or order of the Commission, a covered entity, upon receipt of a subpoena for disclosure of covered information pursuant to legal process, shall, prior to complying, notify the customer in writing and allow the customer 7 days to appear and contest the claim of the person or entity seeking disclosure.

(3) Nothing in this rule prevents a person or entity seeking covered information from demanding such information from the customer under any applicable legal procedure or authority.

(4) Nothing in this section prohibits a covered entity from disclosing covered information with the consent of the customer, where the consent is express, in written or electronic form, and specific to the purpose and to the person or entity seeking the information.

(5) Nothing in this rule prevents a covered entity from disclosing, in response to a subpoena, the name, address and other contact information regarding a customer.

(6) Upon request of the Commission, covered entities shall report to the Commission on disclosures of covered information made pursuant to legal process. The Commission may make such reports publicly available without identifying the affected customers, unless making such reports public is

prohibited by state or federal law or by order of the Commission.

(d) **Disclosure of Information in Situations of Imminent Threat to Life or Property.** These rules concerning access, control and disclosure do not apply to information provided to emergency responders in situations involving an imminent threat to life or property.

20. The principle of data minimization adopted here does not change any existing regulations that currently require the retention of data for periods of time nor does it change any reporting requirements.

21. Adopting the principle of data minimization in this decision does not create a new liability that falls upon utilities and other entities that collect usage data.

22. Since a principle of data minimization is a "best practice" in the protection of the privacy and security of usage data, a principle of data minimization is consistent with SB 1476 and the Pub. Util. Code.

23. The following rules to implement the principle of data minimization are consistent with SB 1476 and the Pub. Util. Code:

5. DATA MINIMIZATION

(a) **Generally**. Covered entities shall collect, store, use, and disclose only as much covered information as is reasonably necessary or as authorized by the Commission to accomplish a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

(b) **Data Retention**. Covered entities shall maintain covered information only for as long as reasonably necessary or as authorized by the Commission to accomplish a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

(c) **Data Disclosure**. Covered entities shall not disclose to any third party more covered information than is reasonably necessary or as

authorized by the Commission to carry out on behalf of the covered entity a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

24. If a third party that obtains customer usage information fails to comply with the tariff provision, the Commission can find the third party ineligible to obtain usage information pertaining to any customer from the utility.

25. The following limitations on the use and disclosure of customer usage data are consistent with SB 1476 and the Pub. Util. Code:

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 electrical corporation may collect, store and use covered information for primary purposes without customer consent. Other covered entities may collect, store and use covered information only with prior customer consent, except as otherwise provided here.

(c) **Disclosures to Third Parties**.

(1) **Initial Disclosure by a Covered Entity**. A covered entity may disclose covered information to a third party without customer consent when explicitly ordered to do so by the Commission or 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 consistent with

applicable program terms and conditions, unless otherwise directed by the Commission.

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

(3) **Terminating Disclosures to Entities Failing to Comply With Their Privacy Assurances**. When a covered entity discloses covered information to a third party under this subsection 6(c), it shall specify by contract that it shall be considered a material breach if the third party engages in a pattern or practice of storing, using or disclosing the covered information in violation of the third party's contractual obligations to handle the covered information under policies no less protective than those under which the covered entity from which the covered information was initially derived operates in compliance with this rule. If a covered entity disclosing covered information finds that a third party to which it disclosed covered information is engaged in a pattern or practice of storing, using or disclosing covered information in violation of the third party's contractual obligations related to handling covered information, the disclosing entity shall promptly cease disclosing covered information to such third party.

(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. This authorization is not required when information is—

(1) provided pursuant to a legal process as described in 4(c) above;

(2) provided in situations of imminent threat to life or property as described in 4(d) above; or

(3) authorized by the Commission pursuant to its jurisdiction and control.

(e) **Customer Authorization**.

(1) **Authorization**. Separate authorization by each customer must be obtained for each secondary purpose.

(2) **Revocation**. Customers have the right to revoke, at any time, any previously granted authorization. Non-residential customers shall have the same right to revoke, unless specified otherwise in a contract of finite duration.

(3) **Opportunity to Revoke**. The consent of a residential customer shall continue without expiration, but an entity receiving information pursuant to a residential customer's authorization shall contact the customer, at least annually, to inform the customer of the authorization granted and to provide an opportunity for revocation. The consent of a non-residential customer shall continue in the same way, unless specified otherwise in a contract of finite duration, but an entity receiving information pursuant to a non-residential customer's authorization shall contact the customer, to inform the customer of the authorization granted and to provide an opportunity for revocation either upon the termination of the contract, or annually if there is no contract..

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

(g) **Availability of Aggregated Usage Data**. Covered entities shall permit the use of aggregated usage data that is removed of all personally-identifiable information to be used for analysis, reporting or program management provided that the release of that data does

not disclose or reveal specific customer information because of the size of the group, rate classification, or nature of the information.

26. Under current federal and state laws, covered entities must notify customers of security breaches.

27. The following rules to promote the quality and integrity of usage data and to ensure the security of data are consistent with SB 1476 and the Pub. Util. Code:

7. DATA QUALITY AND INTEGRITY

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.

8. DATA SECURITY

(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**. A covered third party shall notify the covered electrical corporation that is the source of the covered data within one week of the detection of a breach. Upon a breach affecting 1,000 or more customers, whether by a covered electrical corporation or by a covered third party, the covered electrical corporation shall notify the Commission's Executive Director of security breaches of covered information within two weeks of the detection of a breach or within one week of notification by a covered third party of such a breach. Upon request by the Commission, electrical corporations shall notify the Commission's Executive Director of security breaches of covered information. In addition, electrical corporations shall file an annual report with the Commission's Executive Director, commencing with the calendar year 2012, that is due within 120 days of the end of the calendar year and notifies the Commission of all security breaches within the calendar year affecting covered information, whether by the covered electrical corporation or by a third party.

As a tariff condition, the Commission can require compliance with privacy rules by third parties who obtain usage information from utilities via the internet (also knows as "the backhaul").

28. As a tariff condition, the Commission should limit interconnection between the Smart Meter and HAN-enabled devices that automatically forward usage data to a third party to those third parties who comply with the privacy and security rules adopted in this decision.

29. The following rules are consistent with SB 1476 and the Pub. Util. Code:

9. ACCOUNTABILITY AND AUDITING

(a) **Generally**. Covered entities shall be accountable for complying with the requirements herein, and must make available to the Commission upon request or audit—

(1) the privacy notices that they provide to customers,

(2) their internal privacy and data security policies,

(3) the identities of agents, contractors and other third parties to which they disclose covered information, the purposes for which that information is disclosed, indicating for each category of disclosure whether it is for a primary purpose or a secondary purpose, and

(4) copies of any secondary-use authorization forms by which the covered party secures customer authorization for secondary uses of covered data.

(b) **Customer Complaints**. Covered entities shall provide customers with a process for reasonable access to covered information, for correction of inaccurate covered information, and for addressing customer complaints regarding covered information under these rules.

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

(d) **Audits**. Each electrical corporation shall conduct an independent audit of its data privacy and security practices in conjunction with general rate case proceedings following 2012 and

at other times as required by order of the Commission. The audit shall monitor compliance with data privacy and security commitments, and the electrical corporation shall report the findings to the Commission as part of the utility's general rate case filing.

(e) **Reporting Requirements**. On an annual basis, each electrical corporation shall disclose to the Commission as part of an annual report required by Rule 8.b, the following information:

(1) the number of authorized third parties accessing covered information,

(2) the number of non-compliances with this rule or with contractual provisions required by this rule experienced by the utility, and the number of customers affected by each non-compliance and a detailed description of each non-compliance.

30. The privacy rules adopted in this decision meet the requirements of SB 1476 and existing statutory and regulatory frameworks that protect the privacy of consumers.

O R D E R

IT IS ORDERED that:

1. The Rules Regarding Privacy and Security Protections for Energy Usage Data in Attachment D of this decision are adopted for Pacific Gas and Electric Company, Southern California Electric Company, and San Diego Gas & Electric Company.

2. Within 90 days of the mailing of this decision, Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company must each file a Tier 3 advice letter including whatever tariff changes are necessary to conform its corporate policies concerning customer usage data

to the Rules Regarding Privacy and Security Protections for Energy Usage Data in Attachment D of this decision.

3. Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company must each submit annual privacy reports to the Executive Director, commencing with calendar year 2012, no later than 120 days after the end of the calendar year. These annual reports must contain the information required to be reported annually by Rule 8(b) and Rule 9(c) of the Rules Regarding Privacy and Security Protections for Energy Usage Data in Attachment D of this decision.

4. Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company must each conduct independent audits of its data privacy and security practices, as required by Rule 9(d) of the Rules Regarding Privacy and Security Protections for Energy Usage Data in Attachment D of this decision, and must report the audit findings as part of each general rate case application filed after 2012.

5. Within six months of the mailing of this decision, San Diego Gas & Electric Company must file a Tier 3 advice letter including tariff changes to make price, usage and cost information available to its customers online. The information must be updated at least on a daily basis, with each day's usage data, along with applicable price and cost details and with hourly or 15-minute granularity (matching the time granularity programmed into the customer's smart meter), available by the next day. The tariff changes must offer residential customers bill-to-date, bill forecast data, projected month-end tiered rate, a rate calculator and notifications as the customers cross rate tiers as part of the pricing data provided to customers. The prices must state an "all in" price the customers pay for electricity.

6. Pacific Gas and Electric Company and Southern California Edison Company shall continue to provide customers with price and usage data. Within six months of the mailing of this decision, Pacific Gas and Electric Company and Southern California Edison Company must each file a Tier 3 advice letter including tariff changes to make price, usage and cost information available to its customers online and updated at least on a daily basis, with each day's usage data, along with applicable price and cost details and with hourly or 15-minute granularity (matching the time granularity programmed into the customer's smart meter), available by the next day. The tariff changes must offer residential customers bill-to-date, bill forecast data, projected month-end tiered rate, a rate calculator and notifications as the customers cross rate tiers as part of the pricing data provided to customers. The prices must state an "all in" price the customers pay for electricity.

7. Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company shall each work with the California Independent System Operator in developing a methodology to make wholesale prices available to customers on each company's website, and shall include the provision of wholesale prices in the advice letters required by Ordering Paragraphs 5 and 6 above.

8. Within six months of the mailing of this decision, Pacific Gas and Electric Company and Southern California Edison Company must each file a Tier 3 advice letter including tariff changes that proposes to provide third parties access to a customer's usage data when authorized by the customer. The program and procedures must be consistent with the policies adopted in Ordering Paragraphs 6 and 7 and the Rules Regarding Privacy and Security Protections for Energy Usage Data in Attachment D of this decision.

9. San Diego Gas & Electric Company (SDG&E) must continue to provide third parties access to a customer's usage data when authorized by the customer. Within six months of the mailing of this decision, SDG&E must file a Tier 3 advice letter including tariff changes as need to bring its current program that provides third-party access to a customer's usage data into conformity with the policies adopted in Ordering Paragraphs 5 and 7 and the Rules Regarding Privacy and Security Protections for Energy Usage Data in Attachment D of this decision.

10. Within six months of the mailing of this decision, Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company must each:

a) commence a pilot study to provide price information to customers in real time or near–real time. The pilot study shall be of a size that yields statistically meaningful results.

b) commence a pilot study and trial that permit Home Area Network-enabled devices to be connected directly with Smart Meters. The pilot study and trial shall be of a size that yields statistically meaningful results.

11. The scope of this rulemaking is amended to consider in Phase 2 whether the Rules Regarding Privacy and Security Protections for Energy Usage Data in Attachment D of this decision and other requirements of this decision should apply to electrical corporations in addition to Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company, and to gas corporations, community choice aggregators, and electric service providers.

12. The Executive Director shall cause this Order to be served on all entities identified in Attachment E and the service list for Rulemaking (R.) 10-05-005, R.03-10-003 and R.07-05-025.

13. A party that expects to request intervenor compensation for its participation in Phase 2 of this rulemaking shall file its notice of intent to claim intervenor compensation no later than 30 days after the prehearing conference in this phase of the proceeding or pursuant to a date set forth in a later ruling which may be issued by the assigned Commissioner or Administrative Law Judge.

This order is effective today.

Dated _____, at San Francisco, California.