

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA



FILED

12-17-12
04:59 PM

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

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

**DIVISION OF RATEPAYER ADVOCATES'
OPENING COMMENTS
ON ENERGY DATA CENTER PROPOSAL**

SARAH THOMAS
LISA-MARIE SALVACION
Attorneys
for the Division of Ratepayer Advocates
California Public Utilities Commission
505 Van Ness Ave.
San Francisco, CA 94102
Phone: (415) 703-2310
Email: srt@cpuc.ca.gov

CHRISTOPHER MYERS
Analyst
Division of Ratepayer Advocates
California Public Utilities Commission
505 Van Ness Ave.
San Francisco, CA 94102
Phone: (415) 703-2908
Email: cg2@cpuc.ca.gov

December 17, 2012

TABLE OF CONTENTS

I. INTRODUCTION.....1

II. BACKGROUND3

III. RESPONSE TO RULING’S QUESTIONS5

A. IS A RULEMAKING NECESSARY UNDER CURRENT PRACTICES TO MAKE AGGREGATED AND ANONYMIZED DATA AVAILABLE TO THE PUBLIC? SHOULD THE COMMISSION ESTABLISH AN ENERGY DATA CENTER?5

 1. Is a rulemaking necessary?.....5

 2. Should the Commission establish an energy data center.....5

B. WHAT IS THE VALUE OF AN ENERGY DATA CENTER FOR UTILITY CUSTOMERS AND WHAT COULD THE COST BE?7

 1. What is the value of an energy data center for utility customers?.....7

 2. What could be the cost of a data center?9

C. HOW SHOULD THE ENERGY DATA CENTER BE SET UP? WE HAVE PROPOSED ONE MODEL BUT OTHERS MAY BE POSSIBLE WITHIN THE CONFINES OF STATUTES, RULES, AND CODES. WHAT ARE THE RESPONSIBILITIES OF THE ENERGY DATA CENTER BEYOND PROVIDING AGGREGATED DATA TO UTILITY CUSTOMERS AND THE GENERAL PUBLIC? SHOULD ADDITIONAL RESEARCH AND EVALUATION OF COMMISSION PROGRAMS BE INCLUDED? HOW WOULD THEY DIFFER FROM EXISTING RESEARCH AND EVALUATION BEING CONDUCTED BY THE COMMISSION?12

 1. How should the energy data center be set up?12

 2. What are the responsibilities of the energy data center beyond providing aggregated data to utility customers and the general public?17

D. HOW COULD A DATA CENTER BE FUNDED? CAP-AND-TRADE AUCTION REVENUE ADMINISTRATIVE FUNDS, ELECTRIC PROGRAM INVESTMENT CHARGE FUNDS, ENERGY EFFICIENCY EVALUATION, MEASUREMENT, AND VERIFICATION FUNDS, A NEW SOURCE FROM UTILITY CUSTOMERS?17

E. HOW CAN THE COMMISSION ENSURE THE PROTECTION OF CUSTOMER-SPECIFIC ENERGY USAGE DATA AT THE ENERGY DATA CENTER AND PROVIDE THE NECESSARY OVERSIGHT? ARE CYBER SECURITY REQUIREMENTS NECESSARY? ARE FURTHER GUIDELINES FOR AGGREGATION NECESSARY FOR THE DATA CENTER? IF SO, WHAT SHOULD THOSE SPECIFIC GUIDELINES BE?19

 1. How can the Commission ensure the protection of customer-specific energy usage data at the energy data center and provide the necessary oversight?19

| | |
|------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 2. Are further guidelines for aggregation necessary for the data center? If so, what should those specific guidelines be? | 20 |
| IV. CONCLUSION | 22 |

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)

**DIVISION OF RATEPAYER ADVOCATES'
OPENING COMMENTS
ON ENERGY DATA CENTER PROPOSAL**

I. INTRODUCTION

Pursuant to Rule 6.2 of the California Public Utilities Commission's Rules of Practice and Procedure, the Division of Ratepayer Advocates (DRA) hereby submits these Opening Comments on the *Assigned Commissioner's Scoping Memo and Ruling Amending Scope of Proceeding to Seek Comments and To Schedule Workshops on Energy Data Center* (Ruling), filed on November 13, 2012. The Ruling invites parties to comment on a September 2012 Commission Staff Briefing Paper (Paper or Staff Paper) proposing an Energy Data Center.¹

At best, the proposal is premature, and requires development of a robust record on the need for such a Center, its impacts on customer privacy, and how the privacy implications balance out against that purported need. At worst, the Energy Data Center proposal, if adopted, would allow an unlawful intrusion into customer privacy and should be denied outright.

¹ Ruling, p.1.

Because the Staff Paper refers to aggregate data and customer-specific data interchangeably, it is difficult to tell what data would be released. Clearly, the latter would be unlawful without careful privacy protections. Even if the Paper proposed only release of “aggregated” information, the ability to disaggregate such data is constantly evolving, and therefore the definition of such data must evolve with the technology, as the Commission acknowledged in Decision (D.) 11-07-056.² Further, the “15/15 rule” defining what constitutes aggregated data³ is no longer adequate to protect customer privacy in an age of big data, where data sets are easily disaggregated through triangulation with other data and other means.

Either way, the proposal could result in the wholesale dissemination of valuable and private customer data containing intimate details about the lives and activities of customers the Commission is entrusted to protect. The issue also requires careful consideration and analysis not offered in the Staff Paper.

In summary, DRA makes the following points in these comments (within the questions the Ruling asked):

1. The Commission should first determine if there is a problem and then determine an appropriate solution. Before considering an Energy Data Center, the Commission must develop a record of the need for and privacy implications of a Center, and carefully balance the harm against the purported benefits of such a Center;
2. The proposal assumes that giving data to the “government” is benign, but that assumption may overlook the risk of governmental civil liberties violations, or fail to acknowledge that governments, with limited resources, are not always the best stewards of private information;

² See discussion in Section III.E. 2 below.

³ The old 15/15 rule provides that in order to qualify as “aggregated,” information should be made up of at least 15 customers, and a customer's load must be less than 15% of an aggregation category. If the number of customers in the data is below 15, or if a single customer's load is more than 15% of the total data, further aggregation is required. D.97-10-031, 76 CPUC2d 29 (1997), 1997 Cal. PUC LEXIS 960 at *7.

3. “Aggregated” data means more than it used to – it is much easier to disaggregate now, and the 15/15 rule is no longer viable.
4. The data has high commercial value, and the Commission should consider whether users of the data must pay for it and thereby finance any Energy Data Center;
5. To the extent the Commission has already turned over customer-identifiable data to other governmental entities, the Commission should include information about the nature, purpose and extent of such disclosure in the record of this proceeding.

II. BACKGROUND

The Commission already provided extensive briefing opportunities on the privacy issues relevant to customer data generated by Smart Meters.⁴ For example, DRA (and others) filed comments on March 9, 2010 and October 15, 2010, making clear that California attaches great importance to privacy because – unlike the U.S. Constitution, which has no specific “privacy clause” – privacy is the first principle of the California Constitution:

Privacy is not a luxury or a trivial concern, but a fundamental right enshrined in Article 1, Section 1 of the California Constitution:

SECTION 1. All people are by nature free and independent and have *inalienable rights*. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and *pursuing and obtaining* safety, happiness, and *privacy*.⁵

⁴ An in-depth understanding of the privacy issues is available in comments filed in this docket on or about March 9, 2010 and October 15, 2010, available on the Commission’s website at <http://delaps1.cpuc.ca.gov/CPUCProceedingLookup/f?p=401:57:636129612586101::NO>. DRA especially recommends that those not familiar with the issues review the comments of privacy experts Electronic Frontier Foundation (EFF) and the Center for Democracy and Technology (CDT), filed March 9, 2010, available at <http://docs.cpuc.ca.gov/efile/CM/114696.pdf>, and October 15, 2010, available at <http://docs.cpuc.ca.gov/efile/CM/125121.pdf>.

⁵ *Comments of [DRA] on the September 27, 2010 Assigned Commissioner’s Ruling Soliciting Input on Smart Grid Privacy*, filed Oct. 15, 2010, at 1, available at <http://docs.cpuc.ca.gov/efile/RESP/125117.pdf>.

DRA also invoked U.S. Supreme Court Justice Brandeis' words, in noting that “[t]he right to be left ... alone is as vital today as it was 80 years ago, as Justice Brandeis then observed regarding the essential nature of a right to privacy against governmental intrusion”:

The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, *as against the Government, the right to be let alone -- the most comprehensive of rights and the right most valued by civilized men.* *Olmstead v. U.S.*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (emphasis added).⁶

The Commission acknowledged and accommodated those concerns in D.11-07-056 when it prohibited sharing of customer data without demonstrating compliance with a series of innovative and progressive rules, the Fair Information Practice principles (FIP principles), designed to afford maximum privacy protection to such data.⁷ In so doing, the Commission made clear that to the extent that one can discern specific customer identities or patterns of usage from data, such data does not meet the definition of “aggregated” data, and falls under the definition of “covered data” subject to the adopted privacy protections. Further, as discussed below, the Commission adopted definitions of “aggregated” and “covered data” providing that data subject to the protections must evolve as the ability to disaggregate what might have previously have been considered “aggregated” data evolves.

⁶ *Id.* at 5.

⁷ “In conclusion, this decision adopts the FIP principles as the 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.” D.11-07-056, at 21, available at http://docs.cpuc.ca.gov/published/FINAL_DECISION/140369.htm.

With this background in mind, DRA proceeds to the Ruling’s questions.⁸

III. RESPONSE TO RULING’S QUESTIONS

A. Is a rulemaking necessary under current practices to make aggregated and anonymized data available to the public? Should the Commission establish an energy data center?

1. Is a rulemaking necessary?

DRA is agnostic on whether a separate Rulemaking is necessary, as long as the Energy Data Center receives a full vetting as noted elsewhere in these comments. On the one hand, the parties engaged in this Rulemaking are the most knowledgeable to deal with the privacy issues that the Commission addressed in D.11-07-056, and therefore this proceeding is a good place to address the issue.

On the other hand, it is essential the Commission addresses Energy Data Center proposal fully, including any proposed ratepayer cost to establish the Center. *See* Ruling at 8 (noting that there will be another proceeding to examine “costs and merits of a data center”). The Commission should establish a new proceeding (or phase within this Rulemaking) scoped as a Ratesetting matter with *ex parte* reporting requirements, as it may be difficult to address the privacy issues relevant to such a Center without also considering its “merits,” and “costs,” which the Ruling assumes should be part of a separate proceeding.

2. Should the Commission establish an energy data center

If the Commission is considering setting up an Energy Data Center for *aggregated* data, the Commission should nonetheless create a record on whether it is needed, and if so, guarantee the Center handles only data that is truly aggregated to ensure Commission compliance with privacy law and the rules established in D.11-07-056. DRA agrees with

⁸ DRA does not respond to all questions, but may provide responsive input in reply comments.

the Paper’s concern in the very first sentence – that access to data from the investor owned utilities (IOUs) can be difficult⁹ – but disagrees that the only possible solution is to consolidate the information into a central repository.

Before considering whether an Energy Data Center is needed to house and disseminate *aggregated* data, therefore, the Commission should take the following steps:

- 1) Determine whether there is a problem – e.g., by putting on the record why and how the data is used and by whom; why the Commission has had to facilitate IOU data releases to third parties; other problems that are occurring and how are they resolved; and how the IOUs are interpreting “aggregated” data.
- 2) Determine the least restrictive means to solve the problem, even if it is not an Energy Data Center. For example, the Commission may adopt a standardized definition of aggregated data and set up protocols for IOU release of such data in appropriate circumstances. The new definition of aggregated data would not be the antiquated 15/15 rule, but instead only encompass data that is not – under the current state of technology – susceptible to disaggregation to reveal individualized customer information. This is essentially the definition the Commission used in D.11-07-056 when it adopted rules protecting the privacy of electric usage data.¹⁰ To arrive at a new definition, the Commission should seek evidence on how the current state of data management allows a user to disaggregate what once might have been considered aggregated data. DRA understands that privacy advocates intend to offer data on this issue going forward.
- 3) While considering an Energy Data Center, also consider other transparent processes for the Commission to resolve legitimate third-party complaints regarding access to aggregate data. Such process would not involve off-the-record Commission facilitation of third-party requests, but an on-the-record process that ensures data is only being released for legitimate purposes.

⁹ The Paper’s first sentence states, “*Aggregated customer energy usage information is available, but access to that information is often difficult.*” Paper at 1 (emphasis added).

¹⁰ See Section III.E.2, below.

By engaging in the foregoing analysis, the Commission may well determine that an Energy Data Center is not needed, even for the dissemination of aggregated data.

If the proposal is to set up a Data Center to house and disseminate *customer-specific* data, DRA opposes creation of such an entity. The privacy rules in D.11-07-056 provide strong protections for such data, and customer privacy rights may bar or militate against housing customer-specific data in a centralized repository. Therefore, any proposal to release customer-specific data will require careful examination of how the data will be used, what public interest such uses will serve, and whether any public or ratepayer interest served by disseminating customer data outweighs the privacy intrusions a Center would cause.

B. What is the value of an energy data center for utility customers and what could the cost be?

1. What is the value of an energy data center for utility customers?

The Energy Data Center Paper alludes generally to following possible uses for the data:

- 1) a better understanding of how and when customers consume energy; 2) an evaluation of current programs; 3) the tailoring of energy efficiency and demand response programs; 4) improved planning and maintenance of utility and grid operations; and 5) a better understanding of new varieties of generation or demand response programs and their impacts on the distribution grid.¹¹

Each of these uses – and how Smart Meter data is essential to them – warrants exploration in the record of this proceeding. One of the Smart Grid rulemaking’s handicaps has been the lack of a robust discussion of the changes Smart Meter data will make for each of the enumerated uses – program evaluation, energy efficiency, demand response, grid operation, and new generation, and “a better understanding of how and

¹¹ Paper at 1.

when customers consume energy.” Before arriving at the “solution” of a Data Center, the Commission must consider the problems it is attempting to solve. The Commission should also explain how the data will “enhance energy efficiency,” (or demand response, grid operation, or other uses). The parties most knowledgeable about the data should spell out precisely how the new data will be used, what it will accomplish that is not being accomplished now and at what cost, and whether there are cheaper and easier ways to understand, evaluate and update energy programs. The Commission may wish to invite input from parties to the proceedings for which the Staff Paper indicates the data is most useful.

It is not enough to say “we know the data will be useful and accomplish great things, but it is too soon to know exactly how because the innovation is just starting.” The customer data at issue could be worth billions of dollars to the private market; the monetization of the Internet has come in large part due to the availability of data for marketing purposes. Before customers’ data is given away for free without their knowledge or informed consent, exploration of the reasons for such release must first happen in depth. It may be that such data should never be given away without substantial compensation to individual customers or ratepayers in general. It may be that the only real uses for the data are commercial – as the Paper notes, to “enable third parties to offer additional services directly to customers.”¹² It is far from clear that the Commission’s mandate extends to creation of such opportunities for commercialization.

In the end, the Commission may decide that given the risks of disclosure posed by this broad commercial interest, IOU processing of the data in accordance with current practice is the best option to ensure privacy is protected. The greater the number of institutions and individuals that have access to data, the greater the risk of inadvertent or

¹² Paper at 1.

even intentional disclosure, as evidenced by the daily press barrage about hacking and other unlawful dissemination of private data concerning millions of Americans.

2. What could be the cost of a data center?

DRA questions whether the Commission may lawfully use ratepayer funds to set up an Energy Data Center. There are two components to this objection: first, it may be that the Commission simply lacks discretion¹³ to allocate ratepayer funds to an outside entity to facilitate the exchange of data. The Commission should order briefing on this issue. Second, any allocation of ratepayer funds requires a determination of whether there is a ratepayer benefit to be gained from such funding. Additionally, cost should be part of the consideration of whether a Center is warranted, and that any such proceeding (or phase of a proceeding) should be scoped as Ratesetting in view of the potential for ratepayer cost. The Ruling seems to divorce examination of cost from consideration of whether the Center is a good idea, and DRA disagrees with this approach.

Further, the data may be very valuable if monetized by third parties in order to sell customers new energy and grid management products and services. Thus, any consideration of cost should be a two-way street: the Commission should consider whether ratepayers should receive compensation for use of their data if it is to consider whether ratepayers should fund development of a Data Center.¹⁴

We do not make this assertion idly or cynically. In California, most residential and small business customers have no choice but to take service from IOUs. They therefore make their data available involuntarily. This may not have mattered much before the availability of Smart Meters, because the data was fairly limited in scope. However, as DRA and others pointed out earlier in the Smart Grid proceeding, the data captured by Smart Meters is far more detailed than that available with analog meters.

¹³ See, e.g., Public Utilities Code Section 1757 *et seq.*

¹⁴ Public Utilities Code Section 851 may require such consideration, as it requires gains from certain asset sales to inure to ratepayers' benefit.

The Legislative history of Senate Bill (SB) 1476,¹⁵ which the Commission implemented in D.11-07-056, acknowledged the myriad details revealed by and potential uses of Smart Grid data:

In comments to the CPUC regarding this rulemaking, several privacy groups raised concerns that smart meter systems could reveal intimate and sensitive personal behavior patterns such as when consumers eat, shower, go to bed, wake up, or leave the house. The systems could also detect whether an alarm system is engaged. Related concerns have been raised that smart meter systems could be subject to hacking, leaving consumers vulnerable to identity theft. Many are also concerned that the information collected using a smart meter could be shared with third-party marketers.¹⁶

Several scholarly articles similarly discuss the implications of releasing Smart Meter data:

New Privacy Risks. Granular [Consumer Energy Usage Data] CEUD, when combined with a customer's profile information, may enable the persistent monitoring of individual electricity usage patterns and appliance use. Research indicates that analyzing 15-minute intervals of aggregate household energy can alone pinpoint the use of most major home appliances. This may reveal a *consumer's behavioral patterns, habits, and activities taking place inside the home, including activities like sleeping, eating, showering, and watching TV*. Energy use patterns over time may reveal *the number of occupants in the household, work schedules, sleeping habits, health, affluence, or other lifestyle details and habits*. While utilities could use this information to assist consumers in energy conservation efforts, numerous--and arguably less benign--uses of this data exist outside of the energy management context. This is often referred to as "secondary" uses of data for purposes other than for the provision of electrical power.

¹⁵ Cal. Pub. Utils. Code § 8380 *et seq.* The legislation is available at http://www.leginfo.ca.gov/pub/09-10/bill/sen/sb_1451-1500/sb_1476_bill_20100929_chaptered.html.

¹⁶ Senate Judiciary Committee Bill Analysis for hearing held April 13, 2010, available at http://www.leginfo.ca.gov/pub/09-10/bill/sen/sb_1451-1500/sb_1476_cfa_20100412_120118_sen_comm.html.

Marketers could use granular energy data to make targeted advertisements. Insurance companies could use it to determine premiums (for example, by knowing that a medical device is being used), and landlords to verify lease compliance. Data trackers could trace owners or users of electric vehicles to identify their approximate location and travel history. Criminals could use it to perpetrate fraud, identity theft, or burglary in a confirmed vacant dwelling. Some consumer fear exists that law enforcement could also use the data to identify suspicious or illegal activity and to conduct warrantless surveillance. In a 2010 smart grid survey conducted by the Ponemon Institute, utility customers were the most worried about how the smart grid's collection of personal information would threaten their personal safety and reveal personal details about their lifestyle. According to the Department of Energy (DOE), even if current smart grid technologies cannot yet identify individual appliances and devices in the home in detail, it will certainly be within the capabilities of subsequent generations.¹⁷

¹⁷ D. Rosenfeld, et al., “Third-Party Smart Meter Data Analytics: The FTC’s Next Enforcement Target?,” 12-1 Antitrust Src 2 (Oct. 2012) (citations omitted; emphasis added). *See also* C. Balough, “Privacy Implications of Smart Meters,” 86 Chi.-Kent Law Rev. 161, 176, 190-91 (2011) (discussing possible need for federal legislation to protect privacy of Smart Meter data given current lack of adequate laws and regulations protecting data); K. Doran, “Climate Change and the Future of Energy: Privacy and Smart Grid: When Progress and Privacy Collide,” 41 U. Tol. L. Rev. 909 (Summer 2010) (“[J]ust as more--and more detailed--data about home energy use is pouring into utilities, the information that can be gleaned from that raw data is growing ever higher in resolution. From an electricity usage profile, modern analytical techniques can identify use of specific appliances within the homes, and will in the foreseeable future be able to pinpoint exactly where within the home those appliances are located. *The potential for gleaning potentially private information from this data is truly staggering*, including when a resident showers, watches TV, and how often she prefers microwave dinners to a three-pot meal.”) (emphasis added); Note, “Regulating the Use and Sharing of Energy Consumption Data: Assessing California’s SB 1476 Smart Meter Data Privacy Statute,” 75 Alb. Law Rev. 341, 375 (2011/2012) (“The very real possibility of ratepayer energy consumption data being unevenly regulated by state legislatures and public service commissions demonstrates *the need for a baseline privacy standard set at the national level*. If we acknowledge from the outset that smart grid data will have tremendous value to a myriad of commercial interests, then we must anticipate increasing pressures by third party firms, utilities, and policymakers to allow energy consumption data to be released and leveraged for economic gain) (emphasis added); Note, “Privacy and the Modern Grid,” 25 Harv. J. Law & Tec 199, 202, 224 (Fall 2011) (“To protect individual privacy and ensure consumer trust during the deployment of smart meter technology, it is vital that an individual's smart meter data be protected from suspicionless access by law enforcement,” and “Law enforcement access to an individual's smart meter data will test the durability of the ‘bright line’ that the Fourth Amendment has traditionally drawn at the threshold of the home. . . .”); Note, “Protecting Progress and Privacy: The Challenges of Smart Grid Implementation,” 6 ISJLP 629, 631 (Summer 2011) (“[G]overnment agencies and potentially other parties would appear to have unrestricted access to greater amounts of energy data that may reveal highly personal information. For example, much like how behavioral advertising has evolved through the Internet, a consumer's choices and behaviors could be

These authors conclude that, “At the most fundamental level, consumers should have the right to protect the privacy of their own energy usage data and control access to it.”

The detailed nature of the data – and its potential to confer great wealth on commercial enterprises set up to capitalize on the new data – warrants consideration of whether it has monetary value that should inure to the ratepayers’ benefit. Thus, in considering the “cost” of a Data Center, the Commission should consider whether the cost runs from ratepayers to a Center, or in the other direction. The Commission should not start from the premise that ratepayer funds – or funds that otherwise would revert to ratepayers such as cap and trade revenues, energy efficiency program funding, energy research funding held at the California Energy Commission or other monies – will pay for set-up and ongoing expenses if a Center is created.

C. How should the energy data center be set up? We have proposed one model but others may be possible within the confines of statutes, rules, and codes. What are the responsibilities of the energy data center beyond providing aggregated data to utility customers and the general public? Should additional research and evaluation of Commission programs be included? How would they differ from existing research and evaluation being conducted by the Commission?

1. How should the energy data center be set up?

Again, this question is premature until the Commission makes an on-the-record determination that an Energy Data Center is in the public interest. Without waiving that objection, DRA offers the following thoughts.

collected and analyzed to create a highly detailed profile. This collected information could then be used without the consent of the consumer by advertisers or other, less legitimate parties who seek to gain an advantage over the consumer.”) A search of Lexis/Nexis reveals dozens more articles on the subject.

The premise of the Staff Paper – that “government” is the best place for an Energy Data Center¹⁸ – needs to take into account the risks of governmental possession of private data about millions of its citizens. As former U.S. Supreme Court Chief Justice and California Governor Earl Warren observed four decades ago, “The fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual.”¹⁹

There are two types of risk to governmental possession of private data on its citizens. First, the annals of civil and criminal litigation are full of instances of improper government intrusion into private affairs of the citizenry. The first type of risk, essentially, concerns governmental intrusion into civil liberties, and violation of constitutional rights. The Commission must consider the history of government invasion of privacy using private data of the citizenry as part of this Energy Data Center examination.

Second, but perhaps just as important, the government is not necessarily the best steward of private information where its core mission does not revolve around privacy. In light of this latter problem, DRA understands that the Census Bureau releases “synthetic data” to researchers that mirrors in shape and proportion the actual data, but that contains no “real” data that can be disaggregated to reveal actual private information regarding Americans.²⁰ In any event, the Commission may want to rethink its stance that “government” is the most benign repository of customer information.

It appears the focus on a government home for the Energy Data Center is, at least in part, a result of the Commission’s prior release of customer data to government

¹⁸ See Paper at 2.

¹⁹ The quotation appears in K. Doran, “Climate Change and the Future of Energy: Privacy and Smart Grid: When Progress and Privacy Collide,” 41 U. Tol. L. Rev. 909, *supra* n.17, and comes from Chief Justice Warren’s concurrence in *Lopez v. United States*, 373 U.S. 427, 441 (1963), involving surreptitious tape recording of a live conversation.

²⁰ This practice is described at <http://www.census.gov/icf/docs/synthetic.pdf>.

“research” organizations. (“In limited circumstances, another method for providing customer identifiable data to an organization has been practiced by the Commission when the requests come from the state or local government or other governmental research organizations.”)²¹ Staff concludes, “The Commission can only enter into [Non-Disclosure Agreements] [NDAs] with other governmental organizations.”²² Elsewhere in the Paper, staff states that

Government Code limits the entities that the Commission can enter into NDAs with to other governmental entities. Therefore, the energy data center will have to be a governmental entity. For example, the data center could be part of a University of California campus.²³

Hence, staff presumes that government is the best place to house an Energy Data Center based solely on the Commission’s current practice of giving *customer-specific* data to governmental entities that request it with the sole “privacy protection” being an NDA. Before making this assumption, there should be a record made of past releases of such data to ensure that it has no privacy implications for customers.

Staff states that the relevant provision, Public Utilities Code Section 8380(e)(3) “provides the Commission with authority to direct the release of customer identifiable information without a customer’s consent.”²⁴ Section 8380(e)(3) provides:

This section shall not preclude an electric corporation or gas corporation from disclosing electrical or gas consumption data as required or permitted under state or federal law or by an order of the commission.

However, this section cannot mean that the Commission can simply order wholesale release of customer-specific data to anyone it wishes. If the provision were so

²¹ Staff Paper at 9.

²² *Id.* at 9, n.16.

²³ *Id.* at 3.

²⁴ *Id.* at 23 n.5.

construed, it would mean that the Commission could order production of data to a daily newspaper for publication on its front page. While this is an extreme example, if nothing else, Section 8380(e)(3) must be read to limit such “Commission ordered” uses to those that would not violate the privacy of or otherwise imperil customers.

If not done pursuant to a “Commission order,” or in the course of a “hearing or proceeding” as Section 8380 requires, such release may violate the more generic privacy rule set forth in Public Utilities Code 583,²⁵ which prohibits Commission staff from releasing confidential data to third parties, with misdemeanor penalties for violation. Thus, the Commission does not and should not have the unfettered right to release any data it wishes to governmental third parties.

One author on the privacy implications of government access to Smart Grid data notes the extra risk such access brings, because government may be able to use the data to prosecute the customers to whom it relates without constitutional limitation:

Though several different legal doctrines could potentially apply, existing federal law does not explicitly govern the collection, use, or distribution of advanced metering data *by government agencies*. In *U.S. v. Miller*, the Court determined that Fourth Amendment restrictions on searches do not apply when government agents access

²⁵ Section 583 provides the following:

No information furnished to the commission by a public utility, or any business which is a subsidiary or affiliate of a public utility, or a corporation which holds a controlling interest in a public utility, except those matters specifically required to be open to public inspection by this part, shall be open to public inspection or made public except on order of the commission, or by the commission or a commissioner in the course of a hearing or proceeding. Any present or former officer or employee of the commission who divulges any such information is guilty of a misdemeanor.

Because of the threat of penalty, Section 583 affords comfort to holders of data that their privacy will be protected where appropriate. DRA continues to seek and have trouble obtaining access to certain IOU documents for purposes of its own litigation and analysis, and nothing in these comments should be construed as a waiver of its right to have access to those documents pursuant to Public Utilities Code Section 309.5. Nor should any third party’s right to have access to IOU documents, including customer records, be affected by this proceeding, as long as they seek them through the Commission’s normal discovery processes, or have a statutory or other legal right to such access.

information from third parties. Specifically, the Court allowed prosecutors to enter into evidence the defendant's banking records and account activity acquired from the bank. This is because, according to the Court, *voluntary conveyance of personal information to a service provider invalidates any reasonable expectation of privacy and the information can therefore be accessed by governmental agencies without probable cause.* The Ninth Circuit, following the holding in *Miller*, applied the voluntary conveyance limitation of the Fourth Amendment to electric utility records because, by giving usage information to energy providers, consumers relinquish their subjective assumption of privacy.²⁶

The Energy Data Center proposal fails outright to consider the risks of governmental access to data giving intimate details about millions of Californians. There must be thorough consideration of any constitutional downside of providing detailed Smart Meter data to the “government,” as the staff proposal treats such provision entirely as an upside benefit. While use of the data for government “research” may not pose the same risks as would provision of the data to law enforcement, the Paper does not clearly make this distinction. Staff simply proposes release of data “with governmental organizations that are seeking data for research or operational purposes.”

The Commission must pause to consider the implications of what the staff is proposing. Early missteps in this area could influence policy around the country, as California is – as is often the case – a frontrunner in developing Smart Grid policy. Thus, DRA suggests the Commission take further, specific briefing on the notion of providing detailed customer data to the government, and on whether such action could infringe on the civil liberties of Californians. Further, the Commission should examine the qualifications of any institution in which it would house the data to safeguard the privacy of any data that is susceptible to disaggregation.

²⁶ Note, “Protecting Progress and Privacy: The Challenges of Smart Grid Implementation,” 6 ISJLP 629, *supra* note 17 at 642-43, citing *U.S. v. Miller*, 425 U.S. 435, 446 (1976) and *U.S. v. Starkweather*, 972 F.2d 1347 (9th Cir. 1992) (unpublished table decision).

2. What are the responsibilities of the energy data center beyond providing aggregated data to utility customers and the general public?

As noted above, it is not clear whether the Staff Paper proposes release of aggregated data, specific customer data, or both. The Commission should make clear that any Energy Data Center would only handle *aggregated* data. Before setting up such a Center, the Commission should make a record revealing that the IOUs are not capable of handling the data themselves and that an Energy Data Center would be the best alternative. Only after making these findings should the Commission consider adopting such a Center. If the data were truly aggregated, the key responsibility of an Energy Data Center would be to ensure it is releasing the data to third parties truly interested in improving California's energy usage patterns or other energy-related uses.

If the Commission were to decide that an Energy Data Center should handle customer-specific data, which DRA likely would oppose, the Center's responsibilities would be, at a minimum: 1) having adequately trained staff and sufficient hardware and software to ensure that the Center can protect the privacy of the data, 2) having a duty to protect privacy, with potential liability for negligent or intentional release, and 3) providing consumer notice and credit restoration services in the event of such release.

D. How could a data center be funded? Cap-and-trade auction revenue administrative funds, electric program investment charge funds, energy efficiency evaluation, measurement, and verification funds, a new source from utility customers?

As noted above, including funding in the current inquiry first requires a finding that an Energy Data Center is necessary, that ratepayer funding may lawfully be used to finance it, and that there are adequate privacy protections in place to protect customer data. Further, if the Commission plans to consider funding while it analyzes whether to set up a Center, this proceeding should be re-scoped as Ratesetting.

As for the types of funding the Ruling enumerates, DRA has a few observations. First, the claims on cap and trade auction revenues and the agencies involved in

allocating the money are so numerous that it makes little sense to count on funding from this pot, especially since early revenues are far lower than projected. Energy Efficiency Evaluation, Measurement and Verification (EM&V) funds could possibly be used, if the data were being used to evaluate the performance of specific Energy Efficiency programs, but there is no record here of how Smart Meter data will be used for that purpose. The Electric Program Investment Charge (EPIC) authorized ratepayer funding for research and development, technology demonstration and deployment and market facilitation, but it is not clear that an Energy Data Center would qualify for such funding.²⁷ The Commission would have to examine the cited funding streams and determine if it is within its discretion to use such funding in the proposed manner.

DRA would oppose creation of any new funding source, or use of existing funding sources, without consideration of whether the *recipients* of the data should pay ratepayers for what is clearly very valuable information. As one scholar notes:

Enormous commercial interest surrounds the idea of modernizing the U.S. electric grid via modern digital technology, more commonly known as creating the "smart grid." This interest is evidenced by the staggering amount of capital that continues to flow toward this end. The smart grid market is estimated to grow from \$ 20 billion in 2009, to \$ 42 billion in 2014, and possibly to \$ 100 billion by 2030.²⁸

The data itself carries great commercial value; as one observer notes, "For the third parties, there is big money at stake, and these companies' business models rely on obtaining smart meter data."²⁹ The "surveillance economy" has arrived, and it is worth billions.

²⁷ See D.12-05-037, ordering para. 1.

²⁸ A. Wokutch, "Energy Regulation, The Role of Non-Utility Service Providers in Smart Grid Development: Should They Be Regulated, and if So, Who Can Regulate Them?," 9 J. on Telecomm & High Tech L. 531, 532 (2011).

²⁹ C. Balough, "Privacy Implications of Smart Meters," 86 Chi.-Kent Law Rev. 161, *supra* n.17, at 188.

The Commission has a statutory obligation to ensure that rates are “just and reasonable,”³⁰ and this duty includes consideration of whether ratepayers should receive value for their information, rather than paying others to give away what rightfully belongs to them. If ratepayers had any choice about the gathering of this valuable information on their account, things might be different. Given that they do not, the Commission must first consider having commercial interests pay for the data before it considers any other possible funding source.

E. How can the Commission ensure the protection of customer-specific energy usage data at the energy data center and provide the necessary oversight? Are cyber security requirements necessary? Are further guidelines for aggregation necessary for the data center? If so, what should those specific guidelines be?

1. How can the Commission ensure the protection of customer-specific energy usage data at the energy data center and provide the necessary oversight?

The Commission’s current practice of serving as an intermediary between third parties who want data and the IOUs that possess it is not transparent. DRA requests that the Commission disclose details about these releases as part of its determination of the purported need for an Energy Data Center. DRA requests that the Commission disclose, at a minimum, the following information about its current practice of giving customer-identifiable data to governmental entities based solely on an NDA:

- a. How many such releases have occurred, and over what period;
- b. Whether that data was aggregated or disaggregated;
- c. To whom the Commission turned the data over;
- d. For what purposes the data was requested;
- e. The process for handling the data requests and ensuring data privacy;

³⁰ Cal. Pub. Util. Code § 451, 454.

- f. Any process the Commission has employed to ensure there have been no breaches of privacy with regard to such data, and if there is no such process, how privacy is ensured; and
- g. The legal basis for such releases.

While considering whether to adopt an Energy Data Center, DRA requests that the Commission also consider the alternative of creating its own transparent process for resolving disputes between third parties and IOUs and facilitating access to data. Such a process would be on the record, thereby allowing customers whose data is disclosed and other stakeholders to understand why third parties seek data, how and to whom the Commission has disclosed it, and how privacy is protected.

Finally, any release of customer-specific data requires further protections. The Commission has a duty under Section 583 to ensure that anyone or any entity in possession of or given data that is capable of disaggregation 1) has adequately trained staff and sufficient hardware and software to protect the privacy of the data, 2) has a duty to protect privacy, with potential liability for negligent or intentional release, and 3) provides consumer notice and credit restoration services in the event of such release. Only by bearing these obligations is there an incentive to truly protect customers' privacy.

2. Are further guidelines for aggregation necessary for the data center? If so, what should those specific guidelines be?

In recognition of the changing nature of data to easy disaggregation, any guideline must be fluid. The Commission definition in D.11-07-056 may accomplish this goal; it notably does *not* adopt a 15/15 provision, but simply provides that if the data discloses “specific customer information because of the size of the group, rate classification, or nature of the information,” it is not aggregated data:

- 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.³¹

The wording of the definition suggests that it was intended to evolve as the ability to disaggregate data evolves, since it states that aggregated data “does not” – in the present tense – “disclose or reveal specific customer information.” Thus, it would appear the definition hinges on available methods of disaggregation at the time of the data’s release. Lest there be any doubt, DRA proposes the definition of aggregation include the following phrase: “Aggregated data is data that is not susceptible to disaggregation using methods commonly available at the time of production of the data.”

Further evidence that the definition of aggregated data must evolve with the technology of disaggregation appears in the definition of information covered by the FIP principles as adopted in D.11-07-056:

1. (b) **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* an individual, family, household, residence, or non-residential customer, except that covered information does not include 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*. (D.11-07-056, *mimeo.* at 40; emphasis added.)

As computational techniques get better and better, the meaning of the phrases "can reasonably be used to identify" and "cannot reasonably be identified or re-identified" will change. Thus, D.11-07-056 already contains a narrow definition that must be extended to any Energy Data Center, perhaps with even more specific guidance.

As a consequence, the Staff Paper conclusion that “Aggregated data that does not contain personally-identifiable information, is not subject to the Commission’s Privacy

³¹ D.11-07-056, http://docs.cpuc.ca.gov/published//FINAL_DECISION/140369.htm, at 87.

Rules, nor is an NDA required to obtain such information” must be read in light of D.11-07-056’s narrow definitions of aggregated data and data covered by the FIP principles. To the extent the Paper’s authors would propose a Center that houses customer-specific information or data capable of disaggregation, it would run afoul of the Commission’s adopted rules and should therefore not be approved.

IV. CONCLUSION

For the reasons stated above, the Commission should:

- 1) Develop a record of the need for and privacy implications of an Energy Data Center, and carefully balance the harm against the purported benefits of such a Center;
- 2) Determine that an Energy Data Center is the best way to handle Smart Meter data, and make clear that it will not handle customer-specific data;
- 3) Examine whether a governmental entity is necessarily the best place to house the data;
- 4) Disclose details about Commission releases to date of customer-specific data to third parties;
- 5) Explore whether ratepayers should be compensated for any data revealed to third parties via an Energy Data Center;
and either
- 6) Deny approval of an Energy Data Center outright because of its impacts on privacy;
Or
- 7) Limit the data that is housed in an Energy Data Center to data that is truly “aggregated” under current practice.

Respectfully submitted,

SARAH THOMAS
LISA-MARIE SALVACION

/s/ SARAH THOMAS

SARAH THOMAS

Attorneys for the Division of Ratepayer
Advocates

California Public Utilities Commission
505 Van Ness Ave.
San Francisco, CA 94102
Phone: (415) 703-2310
Email: srt@cpuc.ca.gov

December 17, 2012