TJS/jv1 2/27/2013

FILED
02-27-13
01:55 PM

BEFORE THE PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIFORNIA

Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's own Motion to Actively Guide Policy in California's Development of a Smart Grid System.	Rulemaking 08-12-009 (Filed December 18, 2008) Phase III Energy Data Center

ADMINISTRATIVE LAW JUDGE'S RULING SETTING SCHEDULE TO ESTABLISH "DATA USE CASES," TIMELINES FOR PROVISION OF DATA, AND MODEL NON-DISCLOSURE AGREEMENTS

Summary

This ruling establishes the next steps for receiving proposals to ensure the timely provision of energy usage data, particularly when personally identifiable information (PII) is removed, to requestors of data interested in topics of policy interest to California ratepayers, utilities, and policy makers.

Specifically, the ruling schedules a collaborative process for routinizing the provision of data when possible. The ruling seeks several different proposals. First, the collaborative process should identify use cases in which PII data is not involved and propose a process that makes this data available to requestors expeditiously. Second, the collaborative process should identify use cases where PII data is potentially involved and where a model non-disclosure agreement and other protections can permit the provision of data. Finally, the collaborative

process should identify important use cases where PII data may warrant special consideration by the Commission, including non-routine protections.

Procedural Background

In September 2012, the Commission released a briefing paper titled "Energy Data Center."[1] The Briefing Paper noted that as the energy sector joins the information age, much data concerning energy usage data is now available, but that access to that information is often difficult to obtain.

On November 13, 2012, an Assigned Commissioner's scoping memo and ruling, filed in this proceeding, sought comments on the Briefing Paper and scheduled a workshop on the Energy Data Center.[2]

The Commission received opening comments concerning the Briefing Paper on December 17, 2012, from Distributed Energy Consumer Advocates (DECA), Californians for Renewable Energy, Inc., Natural Resources Defense Council (NRDC), San Diego Gas & Electric Company (SDG&E), Southern California Gas Company (SoCalGas), the Local Government Sustainable Energy Coalition, the Division of Ratepayer Advocates (DRA), Pacific Gas and Electric Company (PG&E), Southern California Edison Company (SCE), The Utility Reform Network (TURN), the Electronic Frontier Foundation, California Center for Sustainable Energy (CCSE), and California Center for Sustainable

---

[1] "Energy Data Center," a Briefing Paper prepared by Audrey Lee, Ph.D., Energy Advisor to President Michael Peevey, and Marzia Zafar, Interim Director of the Commission's Policy and Planning Division, September 2012 (Briefing paper), available at http://www.cpuc.ca.gov/NR/rdonlyres/8B005D2C-9698-4F16-BB2B-D07E707DA676/0/EnergyDataCenterFinal.pdf

[2] *Assigned Commissioner's Scoping Memo and Ruling Amending Scope of Proceeding to Seek Comments and to Schedule Workshops on Energy Data Center*, November 13, 2012.

Communities (CCSC). On December 18, 2012, the Climate Policy Initiative late-filed comments, which the Administrative Law Judge (ALJ) authorized via e-mail on January 4, 2013.

The Commission received reply comments on January 7, 2013, from TURN, DRA, SCE, PG&E, CCSC, Sacramento Municipal Utility District, CCSE, California Municipal Utilities Association, SoCalGas and DECA.

The Commission held extensive workshops on January 15 and January 16, 2013, at the Commission offices in San Francisco to explore a variety of topics raised by parties in comments and replies.

Workshop Developments

The workshops sought to work towards "a consistent, uniform, transparent process for access to energy data from the investor-owned utilities"[3] and to explore security, legal, economic, and policy issues associated with an energy data center.

The first panel provided an overview of the current process by which entities can obtain access to various forms of non-PII aggregated and anonymous data, as well as the issue of access to other forms of potentially PII through the use of a non-disclosure agreement (NDA) with security protocols. In conjunction with the discussion of NDAs, PG&E provided a template for a model NDA including security protocols that could serve as a starting point for the development of a standard NDA. That template is Attachment A to this ruling.

The second panel included a wide ranging discussion of the benefits of an energy data center and the current uses of data. SCE made the case that there is

[3] Energy Data Workshop Agenda, Rulemaking 08-12-009, January 15, 2013.

no problem currently with the sharing of data. SCE argued that of 192 recent requests for aggregated data from SCE, only 2 had serious problems. SCE's review also found that the most common reason for a delay was an incomplete request, and the norm processing time is 10 days. SCE also noted that 182 of the requests were for climate action plans.[4]

In addition to presentations by those using city-level aggregate data for climate action plans, several parties made the case for access to more granular data as a key to moving forward in energy policy. Specifically, a representative of UCLA's Institute for the Environment noted that to better understand the environmental performance of commercial buildings, it was necessary to link energy data to building characteristics and patterns of building use. She argued that a study showed that newer buildings, despite being subject to stricter regulations that seek to promote energy efficiency, appear to use more energy than older buildings. The representative argued that this type of insight required access to granular data. In addition, she argued that it was not the role of the utility to do this kind of analysis, but that it was extremely difficult for university-based researchers to get access to granular data from utilities.[5]

Similarly, a panelist who works as an energy consultant noted that the ability to provide new energy services, such as storage or solar service, in an economic and efficient way requires access to highly granular, yet anonymous, load data. For solar service, the difficulty of getting data adds costs to the design

---

[4] The Commission made a formal data request to utilities concerning third parties' requests for energy data, and the response of each utility is currently under review.

[5] The results of this research will be made public on March 25, 2013 and the Commission has invited the UCLA researchers to present the results on April 3, 2013.

and installation of solar panels. In a similar vein, a panelist argued that to offer a subscription charging service to electric vehicle owners, entrepreneurs require access to highly granular, yet anonymous, data to determine if such a service makes financial sense.

In addition, a representative of the Energy Institute at the University of California, Berkeley, noted that researchers need highly individual yet anonymous or non-PII data to understand electricity consumption behavior. Moreover, to understand the cost effectiveness of energy efficiency programs, access to individual, anonymous data is critical, and obtaining access is currently difficult.

A representative of the California Energy Commission (CEC) noted that the CEC has held data and protected it for over 30 years. She noted that access to energy consumption data is difficult to obtain. Moreover, such access, in her view, is critical for understanding the difference between forecasted benefits and realized benefits of energy policies that have been adopted and implemented by either the CEC or this Commission.

A representative of NRDC noted that financers and lenders need access to aggregate data on the energy use of individuals to determine financial risk for energy efficiency loan products. He noted that the financial community has detailed information on customers' financial and credit history, and expects similar access to data on energy use.

The third panel, on security protocols, provided detailed information on how health information systems are able to use individual data on health to develop general health policies and epidemiological studies, yet are able to protect privacy. In particular, the workshop obtained information on the California Health Interview Survey (CHIS) and a presentation by the information

security officer of UCLA Health Policy Research. At CHIS, access to data comes in three forms, 1) a query system that provides broad access to aggregate data, 2) public use files for individual, anonymous (non-PII) data, and 3) a data enclave for special access to data with PII. This provides different levels of access to the data, making it possible for casual explorations by the public but enabling qualified researchers access to more granular data.

A representative of the Geography Department of the California U.S. Census Research Data Center described the procedures and protocols that the Census Bureau has in place to permit researchers access to granular data with PII at the individual level while still ensuring that all data and studies that are publicly released present only aggregate and anonymous data that do not contain PII. The procedures described include a priori limitations on access to data and its uses. In addition, the Census Bureau provides access to data at specific physical locations, prohibits the use of electronic devices in the data centers, and uses software that monitors the keystrokes of the researchers and tracks which files are accessed. Furthermore, the Census Bureau uses a process that ensures that a review by the Census Bureau precedes any public release of data. The Census Bureau representative described how trust in the confidentiality of census data is "mission critical" to the Census Bureau and how the Census Bureau takes exceptional steps, both to provide access to granular data with PII and to ensure that the privacy of individuals is protected.

The fourth panel focused on privacy principles and standards. Of particular interest were presentations that showed how data resulting from certain types of aggregation or anonymization algorithms can be "reverse engineered" to violate individual privacy, as well as research that showed how

more advanced algorithms could aggregate and anonymize data in ways that are more difficult or impossible to "reverse engineer."

The fifth panel explored the types of problems that a data center can confront when collected data is not standardized and in very different formats – excel, portable document format, floating point decimal, or fixed decimal – and the type of work needed to bring the data together into a usable format.

The sixth panel looked at the issue of providing (non-PII) aggregate and anonymous data. CCSE explained the difference between aggregate data and anonymous data using the Commission's California Solar Statistics program as an example, and explained the benefits of using census blocks as a level for aggregation in ways such that PII was protected. A representative of the Strategic Growth Council demonstrated a relatively simple spatial index algorithm used to aggregate data and protect PII consistent with a model rule, such as the 15-15 rule.[6] DECA argued from the perspective of a small non-governmental organization with limited resources for access to anonymous (non-PII) data to inform energy procurement and other policy decisions. DECA believes that individual customer data can be protected through anonymization and a geographic density filter. SDG&E indicated that in its experience, those wanting data tended to have specific needs that are difficult to anticipate in advance. Thus, even apparently simple requests can require substantial work.

At the conclusion of the workshop, the final session focused on "next steps" and ideas for determining the path forward. SDG&E and SoCalGas

[6] The 15-15 rule states that PII data is protected when a data sample contains more than 15 customers and no single customer's data comprises more than 15 percent of the total aggregated data.

presented a plan to utilize a collaborative workshop process, including a professional facilitator, to better define the top ten energy sharing "use cases." The collaborative process would include the utilities and other parties, as well as subject matter experts to develop the specific data needs of the researchers and to propose privacy protections appropriate to the data for each of the use cases and a common nomenclature for describing the issues and data requirements. The work of the collaborative would be summarized in a report.

Next, under the SDG&E/SoCalGas proposal, the collaborative groups would work with the Commission to streamline the provision of data in ways that continue to protect customer privacy. SDG&E and SoCalGas anticipate that this process will include the development of clear criteria for the sharing of data, the development of security protocols for sharing, storing, handling and disposal of customer information, the development of common non-disclosure agreements and a service level agreement that sets expectations about the receipt of data.

Data: PII, non-PII, Granular, Aggregated

Concerning energy data, the presentations suggested that energy data can be usefully described along two dimensions: whether the data is PII and the level of aggregation in the data. The development of policies to address the different combinations of these data dimensions will produce a comprehensive policy on the availability of data.

Considering the dimension of PII, even though data frequently starts out as a measure of the consumption of a particular business or household, energy data can be non-PII for a number of reasons. In some cases, the data can be so aggregated that it is not possible to determine information about any individual.

An example of this would be data on average per capita statewide electricity use, which provides no information on the use of a specific individual.

Other data can be granular but be grouped into larger sets of data that may reduce the ability to identify specific individuals. For example, an entire set of individual customer energy usage data for the county of Alameda could be removed of all PII such as name or address. On the other hand, if this data set containing individual consumption data also contained individual data on housing characteristics or location, it may prove possible, through the use of other public data sets, to link the consumption data to specific individuals.

At the workshops, the Commission learned that there are steps and algorithms that seek to preserve granular data and provide access to the data, but furnish the information in an anonymous form that shields PII. Unfortunately, even when this is done, it is sometimes possible to "reverse engineer" the algorithm and thereby link data to individuals. A famous recent case of reverse engineering occurred when NetFlix released an anonymous data set of 100,480,507 ratings that 480,189 users gave to 17,770 movies. The data consisted of a user number, movie, date of movie grade, and grade. NetFlix sponsored a contest in which researchers sought to develop movie rating algorithms that seek to predict the grades that customers, based on past grading actions, would give to other movies.

Despite NetFlix's efforts to create an anonymized data set, two researchers at the University of Texas were able to identify individual users by matching the NetFlix data set to film ratings made by individuals that were available on the Internet Movie Database. This led to a lawsuit for violation of the Video Privacy Act.

In the workshops, it was noted that if a data set reveals a person's zip code, birthdate and gender, there is an 87 percent chance that the person can be uniquely identified.

On the other hand, at the workshop there were also presentations showing that is was possible to preserve the anonymity of granular data collected at the individual level. The workshop presented two approaches for the preservation of the anonymity of data. Ashwin Machanavajjhala, Assistant Professor, Computer Science, Duke University and Dan Kifer, Professor, Computer Science, Pennsylvania State University indicated that it is possible to use algorithms that anonymize data in ways that preserved much of the value of the data while producing a data set for which it was not possible to identify individuals.

A second approach to the protection of PII was the "data enclave" approach. Under this approach, the data remains at a very granular level, but selected researchers get very limited access to the data and conduct their analysis in data enclaves that prohibit the researchers from removing any data from the data center. Before obtaining access to the data, the researchers must describe their planned research and agree to privacy protections. In addition, both the process of research and the outcomes of the research are reviewed to ensure that they reveal no PII. An example was given in which a data enclave could allow a researcher to analyze the statistical coefficients that estimate the response in energy usage of individuals to changes in price, but would not release descriptive statistics that describe "average use" in any small geographic cell.

A third alternative to protecting PII is the use of a non-disclosure agreement, including data security protocols, with the Commission or with a utility in which those receiving data pledge under penalty that they will not disclose any PII data and that they have procedures in place to protect the data.

The Commission and utilities have taken this approach when sponsoring studies that concern topics of utility or policy interest that are undertaken by researchers subject to Commission or utility oversight.

These dimensions of data shape situations in important ways. In some situations, such as those involving energy data that is non-PII that and highly aggregated, the investigation of energy policy issues may not raise privacy issues, but instead raise issues associated with managing a process of providing access to data. In situations involving granular data, then issues involving privacy protections and the steps needed to ensure that the data remains non-PII can dominate the policy discussions. In situations that directly involve PII data, then issues concerning privacy will likely dominate policy discussions.

Definitions

The Commission and the California legislature have already completed substantial work on setting rules and policies concerning data aggregations, confidentiality, and uses of information. To facilitate the development of policies that provide easier access to data while protecting privacy, the workshop discussions indicated that there is a need to ensure that there is a common understanding of the key terms used to describe data. This section identifies key terms and begins the process of producing definitions.

In the Commission-adopted privacy rules, the Commission states:

> Privacy Rule Sec. 6(g): (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.

Concerning privacy, the PU Code, states:

> Sec. 394.4(a) Confidentiality: Customer information shall be confidential unless the customer consents in writing. This shall encompass confidentiality of customer specific billing, credit, or usage information. This requirement shall not extend to disclosure of generic information regarding the usage, load shape, or other general characteristics of a group or rate classification, unless the release of that information would reveal customer specific information because of the size of the group, rate classification, or nature of the information.

Concerning anonymized data, the PU Code states:

> Sec. 8380(e)(1): Nothing in this section shall preclude an electrical corporation or gas corporation from using customer aggregate electrical or gas consumption data for analysis, reporting, or program management if all information has been removed regarding the individual identity of the customer.

To date, rules and statutes have focused on "aggregated" data and not on "anonymized" data. Nevertheless, based on the guidelines noted above, a generic definition of anonymized data appears to be possible based on the requirements outlined in statutes and rules. This ruling proposes the following definitions:

> **Aggregated data** means a group or set of data points containing a sufficient number of points removed of personally-identifiable information where one cannot reasonably re-identify an individual customer based on, for example, usage, rate class, or location.
>
> **Anonymized data** means a data set containing individual sets of information where all identifiable characteristics and information, such as, but not limited to, name, address, account number, or social security number, are removed (or scrubbed) so that one cannot reasonably

re-identify an individual customer based on, for example, usage, rate class, or location.

Any adopted methodology for aggregating and anonymizing data should be reviewed periodically to ensure that customer privacy is being maintained. This review process should include a review of existing literature, and engagement with the scientific community and industry to test the methodology.

Based on the presentations and the consideration of law and Commission policies, a task of this proceeding should be a Commission decision that clearly defines the following:

1. Personally identifiable information.
2. Security protocols for handling and disposing of personally identifiable information.
3. The "validity" or "utility" of a particular request for access to granular data.
4. Anonymous data.
5. Reasonable protocols for sharing granular but anonymous (non-PII) and aggregate data that protects the anonymity of the data.
6. Reasonable protocols for sharing aggregate data to preserve the anonymity of the data.
7. Standards for anonymization that ensure the anonymity of data, protect customer privacy, and prevent the reverse engineering of anonymous data.
8. Standards for data aggregation that ensure the anonymity of data, protect customer privacy, and prevent the reverse engineering of the aggregated data. This would include revisiting the "15-15" guideline and developing a threshold that prevents the reverse engineering of aggregated data.

Proposed Use Cases

As suggested by SDG&E and SoCalGas, a Commission decision that adopts procedures for restricting and/or providing access to energy data by

using a "use case" process, would add clarity to the current situation in ways that would help both utilities and requestors of data. Good procedures would also take into consideration the potential cost of providing the data and identify related research or analysis already being undertaken.

Based on the presentations and on further work with data requestors, the initial use cases that the working group will address should cover the following:

Use Case 1: Local Governments seeking access to aggregate data for use in creating legislatively required Climate Action Plans and implementation of energy efficiency programs.

Use Case 2: Research institutions seeking monthly billing data, which may be PII, to evaluate energy policies, including energy efficiency policies, and publishing results in aggregate, non-PII form.

Use Case 3: Research institutions seeking anonymous, individual hourly energy consumption data with other energy-related characteristics to evaluate energy policies, including energy efficiency programs and rate design, and publis hing results as statistical coefficients. Thus, the data could be PII if it contained sufficient characteristics to permit reverse engineering, but the published results that describe the influence of energy-related attributes on consumption, would not be PII.

Use Case 4: Other governmental entities, like the CEC's Energy Upgrade California Program, seeking energy efficiency program participation data by customer identification number in order to cross-reference this data with other program data, and thereby evaluate government-sponsored, legislatively-mandated programs, while publishing results in aggregate, non-PII form. Thus, this data is highly granular, but non-PII, while may be "reversed engineered," but the published results would be non-PII.

Use Case 5: Environmental non-governmental organizations, like the NRDC, requesting PII customer repayment history and energy consumption pre- and post-retrofit for energy efficiency, to support general financial decision-making on energy-efficiency investments through on-bill financing, and produce results that provide aggregate, non-PII findings that link energy usage to other relevant characteristics (e.g. geography, building characteristics, customer financial characteristics, and financing vehicle). In this case, the data is definitely PII, but the results – a decision whether a particular area, type of building, type of customer, or type of financing is viable – in non-PII.

Use Case 6: Solar installation company requesting monthly energy consumption data energy efficiency and participation in the net energy metering program, aggregated to a geographic area that protects PII, to reduce the product development and engineering costs in order to advance residential and commercial solar installations. In this case, the data, prior to aggregation, is PII, while the results – the identification of areas where solar power is financially feasible – is non-PII.

Use Case 7: Building owners and managers seeking monthly energy consumption by building to conduct building benchmarking analyses pursuant to AB 758 and AB1103, and publishing aggregate, non-PII results. In this case, raw data that is PII would likely be needed, but the results concerning the efficacy of the program, are not PII. Moreover, it may prove possible to anonymize such data via an algorithm.

Use Case 8: Energy efficiency contractor seeking CPUC-released aggregate data, similar to what the California Solar Statistics program releases, but using Energy Upgrade California data and other aggregate energy consumption data, to help validate the quality and value of energy efficiency work. Here, the raw

data studied is likely PII but the program result – the validation of the energy efficiency work – does not necessarily reveal PII. Once again, it may prove possible to apply an algorithm that provides anonymization that cannot be reverse engineered.

A task of the collaborative working group would be to more accurately describe use cases and to assess whether a particular use case raises issues that require resolution. The Commission would then use these "use cases" to review and set privacy policies that are consistent with California law and ensure the protection of customer privacy. The working group would work through each of the use cases to ensure that they are fully detailed and described, to assess the risk to privacy that providing access to data entails, and to project the value to ratepayers that the research can produce, and to estimate the cost of preparing or maintaining the data.

Template for Describing Use Cases in Detail

In reviewing the use cases described in the previous section, it is clear that the Commission, to develop effective policy, needs a common way of describing situations that use data. Based on the recent workshops, the template in Attachment B would offer a systematic way of working through the issues of potential data use cases and should be of use to the collaborative workshops.

Model Nondisclosure Agreement

At the workshops, PG&E presented a model non-disclosure agreement, which includes data security protocols, that it offered as a starting point for discussion on the elements of a non-disclosure agreement that could potentially be used by all California energy utilities or other agencies that provide data to eligible recipients. It is Attachment A. The working group will work to further complete or edit this NDA and the appropriate data security protocols.

Tasks and Schedule for Collaborative Working Groups

The collaborative working group should seek to refine and expand on the use cases outlined above. Specifically, the working group should do the following:

1. Propose definitions for the eight terms referenced in the "definitions" section above.
2. Investigate "use cases," including those outlined above, and, to the extent possible, provide information concerning the use cases using the Template Describing Use Cases in Attachment B. To the extent practicable, the working groups should provide recommendations for expediting the transfer of data in cases that do not raise a privacy concern or in cases where a non-disclosure agreement provides privacy protections. The use case scenarios should also assess whether the data is PII or non-PII, granular but anonymized, or aggregated enough to reasonably preclude identification of personal data.
3. Assess the costs to ratepayers that may result from data requests. Costs include but may not be limited to: preparing the data, adhering to a common process for the requests, data transfer tools and establishing or maintaining data security protocols.
4. Review the non-disclosure agreement and security protocols in Attachment B and modify it as reasonable.

The four major utilities and working group participants should work with a Commission-trained facilitator and, after public meetings on the three topics above, provide the Commission with a "Working Group Report" that answers the questions above to the extent possible and identifies issues that require Commission resolution. The utilities shall file and serve a joint "Working Group Report" on May 15, 2013. Parties may file and serve comments on June 5, 2013. Replies are due June 19, 2013.

IT IS RULED that:

1. Pacific Gas and Electric Company, Southern California Electric Company, Southern California Gas Company and San Diego Gas & Electric Company shall form a working group, including representatives of interested parties, to propose refinements to the eight use cases listed above and develop other uses cases, as needed, following the template included as Attachment B.

2. Pacific Gas and Electric Company, Southern California Electric Company, Southern California Gas Company and San Diego Gas & Electric Company shall form a working group, including representatives of interested parties, to propose definitions for the eight terms listed in this ruling.

3. Pacific Gas and Electric Company, Southern California Electric Company, Southern California Gas Company and San Diego Gas & Electric Company shall form a working group, including representatives of interested parties, to propose refinements to the non-disclosure agreement, including data security protocols, which is Attachment A to this ruling.

4. Pacific Gas and Electric Company, Southern California Electric Company, Southern California Gas Company and San Diego Gas & Electric Company shall file and serve a working group report that summarizes the results of the

collaborative working group in the areas of use cases, definitions, and non-disclosure agreements. The report is due May 15, 2013.

5. Pacific Gas and Electric Company, Southern California Electric Company, Southern California Gas Company and San Diego Gas & Electric Company are encouraged to use the meeting facilitation and mediation services offered by the Administrative Law Judge Division of the Public Utilities Commission.

6. Any party wishing to file comments on the report may do so. Comments are due on June 5, 2013. Reply Comments are due on June 19, 2013.

Dated February 27, 2013, at San Francisco, California.

/s/ TIMOTHY J. SULLIVAN
Timothy J. Sullivan
Administrative Law Judge

ATTACHMENT A

ENERGY USAGE DATA NON-DISCLOSURE AND USE OF INFORMATION AGREEMENT

THIS AGREEMENT is by and between _____ ("Company"), _____, ("Undersigned") authorized employee of Company (together, Company and Undersigned are referred to as the "Recipient"), and PACIFIC GAS AND ELECTRIC COMPANY ("PG&E") on the date set forth below [and terminating on _____]. Undersigned and PG&E agree as follows:

1. Mutual Agreement for Services to Benefit PG&E and Its Customers. For mutual consideration received, PG&E and the Recipient agree that the Recipient will perform certain services and work for the benefit of PG&E and its customers as more specifically described in Exhibit A ("*Scope of Energy Usage Data Research*") to this Agreement.

2. Access to Confidential Information. The Recipient acknowledges that in the course of performing services and work for PG&E as described in Exhibit A *Scope of Energy Usage Data Research*, the Recipient may be given access to certain Confidential Information, which includes (a) the customer account information and information relating to their facilities, equipment, processes, products, specifications, designs, records, data, software programs, customer identities, marketing plans or manufacturing processes or products, (b) any technical, commercial, financial, or customer information of PG&E obtained by Recipient in connection with this Contract, either during the Term or prior to the Term but in contemplation that Recipient might be providing the work or services, including, but not limited to customer-specific or other energy usage and billing data, data, matters and practices concerning technology, ratemaking, personnel, business, marketing or manufacturing processes or products, all of which is information owned by PG&E and which constitutes valuable confidential and proprietary information, intellectual property and/or trade secrets belonging to PG&E, and (c) PG&E Data as defined in Exhibit B, *Confidentiality and Data Security* (collectively, "Confidential Information").

3. Protection of Confidential Information. In consideration of being made privy to such Confidential Information, and of the contracting for the Recipient's professional services by PG&E, the Recipient hereby shall hold the same in strict confidence, and not disclose it, or otherwise make it available, to any person or third party (including but not limited to any affiliate of PG&E that produces energy or energy-related products or services) without the prior written consent of PG&E. The Recipient agrees that all such Confidential Information:

(a) Shall be used only for the purpose of providing work or services for PG&E; and

(b) Shall comply with the privacy and information security requirements in Exhibit B, *Confidentiality and Data Security*, and

(c) Shall comply with all applicable privacy and information security laws and regulations, and

(d) Shall not be reproduced, copied, in whole or in part, in any form, except as specifically authorized and in conformance with PG&E's instructions when necessary for the purposes set forth in (a) above; and

(e) Shall, together with any copies, reproductions or other records thereof, in any form, and all information and materials developed by Undersigned there from, be returned to PG&E when no longer needed for the performance of Undersigned's Work or services for PG&E.

4. Remedies for Breach. The Recipient hereby acknowledges and agrees that because (a) an award of money damages is inadequate for any breach of this Agreement by the Recipient or any of its representatives and (b) any breach causes PG&E irreparable harm, that for any violation or threatened violation of any provision of this Agreement, in addition to any remedy PG&E may have at law, PG&E is entitled to equitable relief, including injunctive relief and specific performance, without proof of actual damages.

5. Termination. This Agreement is subject to termination in the discretion of either party upon thirty days written notice, except that the obligations of the Agreement regarding protection of Confidential Information provided prior to the termination shall continue in full force and effect.

6. Choice of Laws. This Agreement shall be governed by and interpreted in accordance with the laws of The State of California, without regard to its conflict of laws principles.

PACIFIC GAS AND ELECTRIC COMPANY	RECIPIENT
By: _____	Company Name: _____
Name: _____	Authorized Agent: _____
Title: _____	Name: _____
Company_____	Title: _____
Date: _____	Date: _____

Exhibit A

SCOPE OF ENERGY USAGE DATA RESEARCH

1. **Purpose Specification.** Recipient shall conduct the following research using the following energy usage data: [DESCRIBE RESEARCH, SPECIFIC ENERGY USAGE DATA REQUIRED FOR THE RESEARCH, THE BENEFITS OF THE RESEARCH TO THE UTILITY AND ITS CUSTOMERS, AND THE RESEARCH DELIVERABLES].

2. **Transparency and Notice.** [IF CUSTOMER-SPECIFIC ENERGY USAGE DATA OR OTHER PERSONALLY IDENTIFIABLE INFORMATION IS TO BE DISCLOSED TO SUPPORT THE RESEARCH, DESCRIBE WHETHER THE RECIPIENT INTENDS TO PROVIDE NOTICE TO INDIVIDUALS REGARDING THE USE OF PERSONALLY IDENTIFIABLE INFORMATION ABOUT THEM, OR OTHER NOTIFICATIONS PURSUANT TO LEGAL REQUIREMENTS SUCH AS THE CALIFORNIA INFORMATION PRACTICES ACT, AND THE MEANS BY WHICH THE INDIVIDUAL MAY REVIEW THE INFORMATION ABOUT THEM FOR ACCURACY.]

3. **Individual Participation:** [DESCRIBE WHETHER INDIVIDUALS MAY GRANT OR REVOKE ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION ABOUT THEM AS PART OF THE RESEARCH.]

4. **Data Minimization:** [DESCRIBE RECIPIENT'S DETERMINATION OF WHETHER PERSONALLY-IDENTIFIABLE INFORMATION IS NECESSARY TO ACHIEVE THE PURPOSES OF THE RESEARCH, AND WHAT METHODS THE RECIPIENT IS USING TO MINIMIZE THE AMOUNT OF PERSONALLY IDENTIFIABLE INFORMATION USED IN THE RESEARCH.]

5. **Use and Disclosure Limitations.** [DESCRIBE IN DETAIL RECIPIENT'S LIMITATIONS ON USE AND DISCLOSURE OF THE ENERGY USAGE DATA, INCLUDING LIMITATIONS AND CONTROLS ON DISCLOSURE TO OTHER THIRD-PARTIES SUCH AS CONTRACTORS, OTHER GOVERNMENTAL AGENCIES, EMPLOYEES, OTHER RESEARCHERS, ETC.]

6. **Date Quality and Integrity.** [DESCRIBE IN DETAIL RECIPIENT'S QUALITY CONTROL AND QUALITY ASSURANCE PROGRAMS TO ENSURE THAT THE DATA IS ACCURATE AND COMPLETE.]

7. **Data Security.** [DESCRIBE IN DETAIL RECIPIENT'S INFORMATION SECURITY PROGRAM AND CONTROLS, INCLUDING ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS TO PROTECT ENERGY USAGE DATA FROM UNAUTHORIZED ACCESS, DESTRUCTION, USE, MODIFICATION OR DISCLOSURE, INCLUDIING COMPLIANCE WITH EXHIBIT B AND ALL APPLICABLE PRIVACY AND INFORMATION SECURITY LAWS AND REGULATIONS.]

8. **Accountability and Auditing.** [DESCRIBE IN DETAIL RECIPIENT'S PROGRAMS AND CONTROLS FOR (A) FOR ADDRESSING COMPLAINTS REGARDING USE OF PERSONALLY IDENTIFIABLE INFORMATION; (B) TRAINING OF ALL EMPLOYEES, AGENTS AND CONTRACTORS WHO USE, STORE, OR PROCESS ENERGY USAGE DATA; AND (C) CONDUCTING PERIODIC INDEPENDENT AUDITS OF ITS DATA PRIVACY AND INFORMATION SECURITY PRACTICES.]

Exhibit B

CONFIDENTIALITY AND DATA SECURITY

1. In addition to the requirements set out in this Agreement and Exhibit A, Recipient shall comply with the following additional terms of this Exhibit B (Confidentiality and Data Security) regarding the handling of Confidential Information and PG&E Data from PG&E or its Customers.

2. **Non-disclosure Agreements:** Recipient shall have all of its employees, SubRecipients, and SubRecipient employees who will perform work or services under this Contract sign a non-disclosure agreement in the same form as this Agreement. Prior to starting said work or services, Recipient shall promptly furnish the original signed non-disclosure agreements to PG&E.

3. **Security Measures:** Recipient shall take "Security Measures" with the handling of Confidential Information to ensure that the Confidential Information will not be compromised and shall be kept secure. Security Measures shall mean industry standards and techniques, physical and logical, including but not limited to:

   a. written policies regarding information security, disaster recovery, third-party assurance auditing, penetration testing,
   b. password protected workstations at Recipient's premises, any premises where Work or services are being performed and any premises of any person who has access to such Confidential Information,
   c. encryption of Confidential Information, and
   d. measures to safeguard against the unauthorized access, destruction, use, alteration or disclosure of any such Confidential Information including, but not limited to, restriction of physical access to such data and information, implementation of logical access controls, sanitization or destruction of media, including hard drives, and establishment of an information security program that at all times is in compliance with the industry requirements of ISO 27001.

4. **Compliance and Monitoring:** Recipient shall comply with security policies relating to the handling of Confidential Information.

   a. Prior to PG&E's first transfer of Confidential Information to Recipient, Recipient shall provide PG&E with documentation satisfactory to PG&E that it has undertaken Security Measures.
   b. Recipient and PG&E agree to meet periodically, if requested by PG&E, to evaluate Recipient's Security Measures and to discuss, in good faith, means by which the Parties can enhance such protection, if necessary.
   c. Recipient shall update its Security Measures, including procedures, practices, policies and controls so as to keep current with industry standards, including but not limited to NIST and NERC/CIP, as applicable.
   d. PG&E reserves the right to perform onsite security assessments to verify the implementation and ongoing operation and maintenance of security controls. At least annually, Recipient shall assist PG&E in obtaining a copy of any report that documents Recipient's Security Measures.
   e. In the event, PG&E determines Recipient has not complied with Security Measures, PG&E shall provide written notice to Recipient describing the deficiencies. Recipient shall then have sixty (60) calendar days to cure. If Recipient has not cured the deficiencies within sixty (60) calendar days, PG&E may cancel this Contract for cause in accordance with Article 40.0 of these General Conditions.

5. **PG&E Data:** PG&E Data shall mean:

   a. all data or information provided by or on behalf of PG&E, including, but not limited to, personally identifiable information relating to, of, or concerning, or provided by or on behalf of any Customers,
   b. all data or information input, transferred, uploaded, migrated, or otherwise sent by or on behalf of PG&E to Recipient as PG&E may approve of in advance and in writing (in each instance),

c. account numbers, forecasts, and other similar information disclosed to or otherwise made available to Recipient by or on behalf of PG&E and Customers, and

d. all data provided by PG&E's licensors, including any and all survey responses, feedback, and reports, as well as information entered by PG&E, Recipient or SubRecipient, and Participating Customers through the Program.

6. **Security of PG&E Data:** Recipient agrees that Recipient's collection, management and use of PG&E Data during the Term shall comply with these security requirements and all applicable laws, regulations, directives, and ordinances.

a. Vendor Security Review: Before receiving any PG&E Data, Recipient shall undergo PG&E's Vendor Security Review process. Recipient may receive PG&E Data if Recipient receives a risk rating of 3, 2 or 1 from PG&E at the conclusion of the PG&E Vendor Security Review process. If Recipient receives a risk rating of 4 or 5 from PG&E, Recipient may not receive PG&E Data until such time Recipient receives a risk rating of 3, 2 or 1.

7. **Use of PG&E Data:**

a. License: PG&E may provide PG&E Data to Recipient to perform its obligations hereunder. Subject to the terms of the Contract, PG&E grants Recipient a personal, non-exclusive, non-assignable, non-transferable limited license to use the PG&E Data solely for the limited purpose of performing the Work or services during the Term, but not otherwise.

b. Limited Use of PG&E Data: Recipient agrees that PG&E Data will not be (a) used by Recipient for any purpose other than that of performing Recipient's obligations under this Contract, (b) disclosed, sold, assigned, leased or otherwise disposed of or made available to third parties by Recipient, (c) commercially exploited by or on behalf of Recipient, nor (d) provided or made available to any other party without written authorization, subject to these General Conditions and Exhibit 5 and Exhibit 6.

c. Application Development: Recipient agrees that it will not engage in any application development without or until it has demonstrated compliance with the provisions of these General Conditions and Exhibit 5 and Exhibit 6.

8. **Security Breach:** Recipient shall immediately notify PG&E in writing of any unauthorized access or disclosure of Confidential Information and/or PG&E Data.

a. Recipient shall take reasonable measures within its control to immediately stop the unauthorized access or disclosure of Confidential Information and/or PG&E Data to prevent recurrence and to return to PG&E any copies.

b. Recipient shall provide PG&E (i) a brief summary of the issue, facts and status of Recipient's investigation; (ii) the potential number of individuals affected by the security breach; (iii) the Confidential Information and/or PG&E Data that may be implicated by the security breach; and (iv) any other information pertinent to PG&E's understanding of the security breach and the exposure or potential exposure of Confidential Information and/or PG&E Data.

c. Recipient shall investigate such breach or potential breach, and shall inform PG&E, in writing, of the results of such investigation, and assist PG&E (at Recipient's sole cost and expense) in maintaining the confidentiality of such Confidential Information and/or PG&E Data. Recipient agrees to provide, at Recipient's sole cost and expense, appropriate data security monitoring services for all potentially affected persons for one (1) year following the breach or potential breach, subject to PG&E's prior approval.

d. If requested in advance and in writing by PG&E, Recipient will notify the potentially affected persons regarding such breach or potential breach within a reasonable time period determined by PG&E and in a form as specifically approved in writing by PG&E. In addition, in no event shall Recipient issue or permit to be issues any public statements regarding the security breach involving Confidential Information and/or PG&E Data unless PG&E requests Recipient to do so in writing.

9. **Right to Seek Injunction:** Recipient agrees that any breach of this Exhibit B (Confidentiality and Data Security) would constitute irreparable harm and significant injury to PG&E. Accordingly, and in addition to PG&E's right to seek damages and any other available remedies at law or in equity in accordance with this Contract, Recipient agrees that PG&E will have the right to obtain,

from any competent civil court, immediate temporary or preliminary injunctive relief enjoining any breach or threatened breach of this Contract, involving the alleged unauthorized access, disclosure or use of any Confidential Information and/or PG&E Data. Recipient hereby waives any and all objections to the right of such court to grant such relief, including, but not limited to, objections of improper jurisdiction or forum non convenience.

10. **CPUC Disclosure:** Notwithstanding anything to the contrary contained herein, but without limiting the general applicability of the foregoing, Recipient understands, agrees and acknowledges as follows.
    a. PG&E hereby reserves the right in its sole and absolute discretion to disclose any and all terms of this Contract and all exhibits, attachments, and any other documents related thereto to the California Public Utilities Commission (CPUC), and that the CPUC may reproduce, copy, in whole or in part or otherwise disclose the Contract pursuant to its regulatory and legal authority.
11. **Subpoenas:** In the event that a court or other governmental authority of competent jurisdiction, including the CPUC, issues an order, subpoena or other lawful process requiring the disclosure by Recipient of the Confidential Information and/or PG&E Data provided by PG&E, Recipient shall notify PG&E immediately upon receipt thereof to facilitate PG&E's efforts to prevent such disclosure, or otherwise preserve the proprietary or confidential nature of the Confidential Information and/or PG&E Data. If PG&E is unsuccessful at preventing the disclosure or otherwise preserving the proprietary or confidential nature of the Confidential Information and/or PG&E Data, or has notified Recipient in writing that it will take no action to prevent disclosure or otherwise preserve the proprietary or confidential nature of such Confidential Information and/or PG&E Data, then Recipient shall not be in violation of this Agreement if it complies with an order of such court or governmental authority to disclose such Confidential Information and/or PG&E Data.

(END OF ATTACHMENT A)

ATTACHMENT B

1. Overview

1.1 Use Case Summary

< This section would provide a short context for the specific use case and provide the summary of the document.>

1.2 Objectives

<This section should describe what the parties are trying to achieve here, e.g. "analyze customer usage data to better understand effectiveness of the energy efficiency programs".>
ADD SECTION ON VALUE to RATEPAYERS OF USE CASE or place within 1.2 Objectives

1.3 Actors

<This section should describe the participants in this process. At a minimum, this should specify the data owner and the data requestor. This may end up being the same across all of the use-cases, but maybe different.>

Name	*Role description*
Utility Organization	
CPUC	
Academic institution	
3rd party	

1.4 Applicable Statutes and Regulatory Rules

<This section should describe any specific rules or regulations that already apply to this use case, e.g. if there are requirements that stem from a specific CPUC mandated program.>

Agency	*Description*	*Applies to*
CPUC		
Other		

2. Use Case Details

2.1 Current Data Practices

<This section can quickly summarize how the process for this use case takes place today. It can be helpful in getting people grounded.>

2.1 Requested Data Practices

<This section should focus on the desired "to-be" state, without necessarily spelling out the technical solution. In other words, it should capture the process through which the parties want to interact, but not necessarily the tools and all the policies that need to be in place. If consensus can't be reached, this section can summarize the options.>

3. High Level Requirements

3.1 Data Granularity Requirements and Data Use

<This section should summarize the type of data that we are talking about for this specific use case. Not every data element should be spelled out at this level – just the type/categories of data.>

Data Type	*Priority (H/M/L)*	*Aggregated/Anonymized/Identifiable*	*Description/Additional Comments*
e.g. 15 minute interval usage data	H	Identifiable	Data that's being recorded by a customer's meter at a 15 minute interval. Etc…

3.2 Data Collection and Maintenance Requirements

<This section should outline high-level functional requirements (technical and non-technical). For example, any requirements about how frequently data needs to be updated, what format it needs to be in, security specifications etc.>

Requirement	*Priority (H/M/L)*	*Additional Comments*
e.g. The data shall include consumption information in kWh for the past 6 months	H	This data is critical because….

3.3 Required Policy & Other Determinations

<*This section should outline high-level policy requirements, e.g. if there is a need to have CPUC approve release of data. Anything else should also go here.*>

Requirement	*Priority (H/M/L)*	*Additional Comments*
e.g. The CPUC shall approve the release of any data that could be personally identifiable	H	

4. Current Data Obstacles and Other Issues

4.1 Barriers

<This section should summarize all the barriers that currently exist or are anticipated by the stakeholders.>

Barrier Description	*Priority (H/M/L)*	*Current/Anticipated*

4.2 Outstanding Issues

<This section should summarize any issues or open questions that the team wasn't able to resolve.>

Description	*Proposed Next Step, if any*
e.g. there wasn't enough information about how XYZ is being done today	

4.3 Additional Comments

<Anything that didn't fit anywhere else can go here.>

5. Conclusion

5.1 Conclusion

<Conclusions about this use case.>

5.2 Recommended Next Steps

<*Proposed next steps.*>

Appendix

Contact

<*May want to include the list of people who participated in the development of the use case or who to contact with questions.*>

Reference Materials

<*Reference Materials.*>

(END OF ATTACHMENT B)