

# Existing Energy Data Sharing Protocols: A Potential Consensus Approach

**Christopher J. Warner**  
**Chief Counsel**  
**Pacific Gas and Electric Company**  
**CPUC Workshop – January 15, 2013**



## **3 Steps to a Consensus Approach**

- 1. Define the data – Personally identifiable information, aggregated data, or somewhere in between**
- 2. Define the scope of research and customer benefits**
- 3. Define the appropriate privacy, information security and intellectual property protocols**

# Step 1 – What is PII? What is not PII? What is IP? What is not IP?

- **PII:**
  - Legal: CPUC privacy rules, Public Utilities Code Section 8380; Civil Code 1798.3(a)
  - Technical: Information security algorithms, “re-identification” software programs
- **IP:**
  - Government Code Sections 6254(c), 6254.7(d)
  - Common law; business practices

## Step 2 – What is the proposed use of the data and scope of research?

- **PG&E “Category 1” and CPUC Privacy Rules “primary purposes”:**

Use of data to directly support public utility services to customers, such as energy efficiency programs, or legally mandated disclosures, such as to law enforcement agencies, local government tax agencies, or Community Choice Aggregators pursuant to state or federal law or court-ordered subpoenas

- **PG&E “Category 2” and CPUC Privacy Rules “secondary purposes”:**

Use of customer-specific data pursuant to express customer authorization, such as through tariffed customer consent forms, “Green Button,” “My Account.”

- **PG&E “Category 3”:** Uses of customer-specific data and aggregated data not included under Categories 1 and 2, such as energy data research

## Step 3 – Privacy, security and IP protocols

- **PII:** FIPPs, CPUC Privacy Rules, Public Utilities Code 583 and 8380, Civil Code 1798 *et seq.* (California Information Practices Act), Business and Professions Code 22575-22579 (California Online Privacy Protection Act), CPUC General Order 66-C and D.06-06-066 (“Confidentiality Matrix”)
- **Information Security:** CPUC Privacy Rules, Public Utilities Code 8380(d) (“reasonable security procedures and practices”), “best industry practices” in information security and cyber-security
- **IP:** Public Utilities Code 851 restriction on transfer of utility assets; California “trade secrets” laws and precedents

# How do we translate into standard data research sharing agreement?

## “Strawperson” sample agreement provisions:

- Standard NDA language
- Standard information security protocols, including (a) prior review of security program and controls, (b) notification of breach, and (c) controls on subcontractors, employees and agents
- Scope of work defined to identify (a) specific data to be shared, (b) mutual benefits and research “deliverables” for utility customers, and (c) appropriate notice to customers if PII shared (“purpose specification” and “notice”)

# Conclusion

*Customer privacy and customer data sharing are not a “zero sum;” appropriate standard protocols and agreements can be implemented that maximize the availability of energy data for public purpose research while appropriately protecting customer privacy and utility assets.*