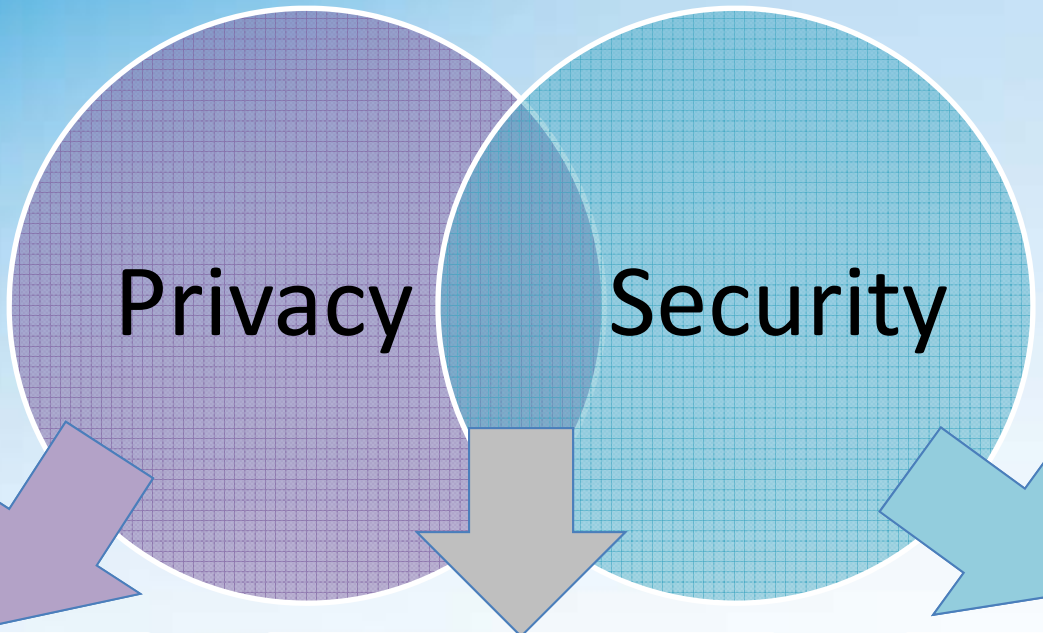
CPUC Datacenter Workshop

January 15, 16 2013

Christopher Vera, GLEG, GCFA, CISSP
Office of Customer Privacy
San Diego Gas & Electric

Customer Privacy & Information Security



- Are we doing what we said we would with customer data?
- Are we giving our customers choices regarding their data?
- Can customers see their data & request corrections?
- Is the data accurate?

- Are we protecting sensitive customer data?
- Are we properly disposing of customer data?
- Does the data have high integrity?
- Are we in compliance with privacy law & regs?

- Are we adequately protecting company information?
- Are we in compliance with security law & regs?

Why Energy Privacy?

- Perceptions of privacy continue to change
  - Paradigm-changing technologies like the Internet **impacted privacy** in ways we could have scarcely imagined 30 years ago
  - Today, Smart Grid technologies like smart meters are **changing the way we look at energy privacy**
- We know customers expect it
  - "SDG&E understands that the full benefits of Smart Grid **cannot be achieved** if it does not have the **confidence** of the users of the system." (SGDP, pg. 139)

- It's the **right thing to do**
- Regulators require it
  - CPUC Decision 11-07-056 – Electricity Usage Data Privacy Decision **applies strict rules** around how customer privacy is respected and protected

Example Smart Grid Privacy Concerns

Energy usage information that SDG&E protects can reveal preferences & behavior

What can be seen now

- Types & quantity of appliances (i.e., refrigerator, A/C)
- Whether solar panels or electric vehicles are present
- Load trends (when customer is home & when they're not)

…& perhaps in the future

- Make, model, condition of any plugged-in device
- Whether appliances are operating efficiently
- Whether refrigerator is full or empty
- What is watched on TV
- How much time playing XBox

SDG&E's position on privacy

- Privacy is a **fundamental right** of every customer
- **Energy privacy**—privacy around the collection & use of a customer's usage data—is a relatively **new concept** outside utilities that requires extensive awareness & education of risks
- SDG&E sees itself as a steward of customer information & is dedicated in its **obligation** to protect it & our customers' energy privacy
- SDG&E is **committed** to doing its part to **advocate** for energy privacy on behalf of its customers & our community
- SDG&E desires to work **collaboratively** with external partners to find ways to advance its customer privacy program

Maintaining the Trust of Our Customers

SDGE connected
A Sempra Energy utility℠

Smart Grid benefits

Granular information

Smart meters

Without the TRUST of our customers, they may "OPT-OUT" and the full benefits of Smart Grid cannot be achieved.

Privacy by Design: The 7 Foundational Principles

1. ***Proactive*** not ***Reactive***: Preventative, not Remedial;
2. Privacy as the ***Default*** setting;
3. Privacy ***Embedded*** into Design;
4. ***Full*** Functionality: Positive-Sum, not Zero-Sum;
5. End-to-End **Security**: **Full** Lifecycle Protection;
6. Visibility **and** Transparency: Keep it **Open**;
7. Respect for User Privacy: Keep it **User-Centric**.

Privacy by Design

The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles *(see over page)*:

www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

Privacy By Design Applied to Simplified IT Product Lifecycle