Applying *Privacy by Design* Best Practices to SDG&E's Smart Pricing Program

March 2012

SDGE connected

A Sempra Energy utility℠

Information and Privacy Commissioner,
Ontario, Canada

Acknowledgements

The authors of this paper gratefully acknowledge the important contribution of staff at the Information and Privacy Commissioner's Office and San Diego Gas & Electric®. We wish to thank Michelle Chibba, Director of Policy and Special Projects, Catherine Thompson, Regulatory and Policy Advisor, and SDG&E staff responsible for the Smart Pricing Program, Information Technology, Information Security and the Smart Grid.

Information and Privacy Commissioner, Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

Foreword

We are very pleased to present the results of our cross-border partnership to bring *Privacy by Design* (*PbD*) to the Smart Pricing Program at San Diego Gas & Electric® (SDG&E®).

It was not that long ago when federal, state and local government, regulators and utilities began the effort to modernize the electrical grid. Recall that at such an early stage, there wasn't even a common definition for what was meant by Smart Grid. Nonetheless, the aging electrical grid needed to be updated and made smarter in order to address growing energy requirements, in an environmentally sustainable manner. Our interest, however, relates to the infrastructure that was envisioned to support the modernization of the electrical grid, knowing that it would be capable of collecting detailed information on energy consumption.

At a granular level, an energy use profile in the context of the Smart Grid will become a source of detailed, behavioral information. With a smart metering communication infrastructure, information about specific electric devices in a customer's home will reveal not only the amount of electricity used, but rather, when and how long the device is used, for example. Privacy concerns arise when there is a possibility of revealing personally identifiable information such as the personal lifestyle habits and behaviors of customers, especially if this information is mishandled or used for secondary purposes other than providing electricity.

In Ontario, Canada, there are now over 4.7 million smart meters installed on households; approximately 3.6 million meters already bill using hourly readings under the time-of-use program. Ontario identified early on that privacy in the Smart Grid was a 'sleeper issue' and needed to be addressed as one of the critical success factors to implementing the Smart Grid. We are proud of our track record in raising the issue of privacy in the Smart Grid, having written a number of papers and guidance documents. It is no wonder then, that when SDG&E was embarking on its Smart Pricing Program, it agreed on a partnership with Ontario's Information and Privacy Commissioner (IPC) to take a *Privacy by Design* approach. This is not surprising because at SDG&E, customer privacy is a critical aspect of building and operating a secure, reliable and trustworthy Smart Grid. SDG&E also believes that privacy is a fundamental right of every customer and that the utility is a steward of customer information, with an obligation to protect it. We clearly stated the importance of customer privacy in our Smart Grid Deployment Plan (SGDP) filed with the California Public Utilities Commission (CPUC) on June 6, 2011 and are taking this opportunity to work with the IPC to make sure that privacy requirements are integrated into our plans, right from the beginning. SDG&E is demonstrating its commitment to finding innovative ways to protect the privacy of its customers.

This joint white paper centers on one specific initiative being implemented by SDG&E, its Smart Pricing Program, which will offer new pricing options for residential and business customers, along with the tools needed to help customers better manage their energy use.

SDG&E is not asking why we need to think about privacy considerations but rather how we will make sure that consumer energy use data is managed in a responsible manner so as to maintain the confidence of consumers throughout this modernization of the electrical grid.

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

Caroline Winn
Vice President, Customer Services
Chief Customer Privacy Officer
San Diego Gas & Electric

Table of Contents

Introduction

Utilities and regulators have developed a keen awareness of the importance of proactively building privacy directly into the Smart Grid over the past two years. For example, the U.S. National Institute of Standards and Technology's (NIST) Smart Grid Privacy Working Group endorsed *Privacy by Design* (*PbD*) in their report entitled, "NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid." In addition, the California Public Utilities Commission (CPUC) adopted a comprehensive set of privacy rules related to energy use data in July, 2011 applicable to electric investor-owned utilities (IOUs) in California[1,2] (See Appendix A).

San Diego Gas & Electric (SDG&E) is taking a leadership position to advance the Smart Grid and acknowledges the importance of proactively building privacy into its design, as it plans for the various phases of implementation. As such, SDG&E is collaborating with the Office of the Information and Privacy Commissioner (IPC) of Ontario, Canada, to put into action the policies, approach, and standards to protect the privacy of customer data by working together on SDG&E's Smart Pricing Program. This effort will result in a privacy model and associated deliverables that can be leveraged and further improved as SDG&E implements other projects.

This collaborative initiative is an effort to share how one utility - SDG&E - is incorporating the *PbD* Smart Grid Best Practices into its organization.[3] The paper begins with an overview of key privacy influences, including privacy changes in California, SDG&E's Smart Grid Deployment Plan (SGDP) and the *PbD* approach. The paper then describes SDG&E's efforts towards protecting customers' privacy and the results arising from embedding the *PbD* principles into the early planning stage of the Smart Pricing Program.

1 See SDG&E Application (A.) 11-06-006: http://sdge.com/node/462

2 See California Public Utilities Commission Decision (D.) 11-07-056, attachment D: http://docs.cpuc.ca.gov/PUBLISHED/GRAPHICS/140370.PDF

3 The full *PbD* Smart Grid Best Practices are contained in *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid* available online at www.ipc.on.ca. See also, *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, and *Operationalizing Privacy by Design: The Ontario Smart Grid Case Study*, also available at www.ipc.on.ca. See also the International Working Group on Data Protection in Telecommunications Working Paper *Privacy by Design and Smart Metering: Minimize Personal Information to Maintain Privacy* (13 September 2011).

California's Privacy Vision

There is a term to describe California's consumer and environmental policy influence – the "California effect."[4]

"Top clean tech investment deals in the world read like a who's who of California businesses."[5] As a result, California is a leader in mitigating and reducing its greenhouse gas emissions.[6] In addition, California has clearly shown Smart Grid leadership, "[t]he Golden State is at the top of everyone's list."[7] California was the first state to pass a statewide Smart Grid bill, Senate Bill (SB) 17 which made Smart Grid the policy of the state[8] (See Appendix B).

Within the United States (U.S.), California is also a leader in privacy protection. For example, after California passed its data breach notification law in 2002, nearly every other state in the U.S. followed suit.[9] California was also the first state to introduce laws requiring California businesses to post privacy policies on their websites regarding the personal information given to third parties and how to opt out of such disclosures.[10]

On October 11, 2009, SB 17 was signed into California law and lays out state policy for the modernization of its electrical transmission and distribution system. It tasked the CPUC with determining the requirements for their Smart Grid Deployment Plan (SGDP), consistent with the policies set forth in the bill and federal law. The bill also required investor-owned utilities, such as SDG&E, to develop SGDPs and file them no later than July 1, 2011. These plans were filed, as required and on time, by SDG&E, Pacific Gas & Electric, as well as Southern California Edison.

Following the passage of SB 17, the CPUC issued a decision which included detailed requirements for the SGDPs and ordered SDG&E and others to file the plan as required by law.[11] The decision outlined the required elements of the plan, including: 1. Smart Grid Vision Statement; 2. Deployment Baseline; 3. Smart Grid Strategy; 4. Grid Security and Cyber Security Strategy; 5. Smart Grid Roadmap; 6. Cost Estimates; 7. Benefits Estimates; and 8. Metrics.

The CPUC's decision states that utilities should include information on how to "[e]mpower consumers to actively participate in operations of the grid,"[12] and the promotion of the "smart customer." The smart customer is informed, empowered and able to use electricity efficiently and in ways that promote the achievement of state environmental goals, consistent with SB 17 policies and initiatives.[13] Additionally, the CPUC posed a number of probing questions related to customer privacy practices, both in terms of current practices and going forward, which were addressed in the utilities' SGDPs.

4 Vogel, David. "Trading up and governing across: transnational governance and environmental protection." *Journal of European Public Policy* 4(4), 1997.
5 Floyd, Nancy and Frank, Susan. "Opinion: AB 32 is an investment in stabilizing California's future." *Capitol Weekly* (18 October 2011).
6 EXECUTIVE ORDER S-13-08, Office of the Governor, www.climatechange.ca.gov
7 Berst, Jesse. "Smart Grid Leadership." *www.SmartGridNews.com* (24 March 2009).
8 Ricketts, Camille. "California quietly passes first statewide Smart Grid law." *Venturebeat.com* (27 October 2009).
9 http://www.ncsl.org/Default.aspx?TabId=13489
10 Olsen, Stefanie. "California privacy law kicks in." *CNET* News (6 July 2004).
11 Decision10-06-047, dated June 24, 2010, in Rulemaking 08-12-009
12 *Ibid.* (pg. 31).
13 *Ibid.* (pg. 125).

The scope of what is considered personal information will vary among jurisdictions and specific laws. In California, the scope of personal information protected by CPUC rules extends to any "electrical or gas consumption data," which means data about a customer's electrical or natural gas usage that is made available as part of an advanced metering infrastructure, and includes the name, account number, or residence of the customer.[14]

14 Public Utilities Code Section 8380(a); *see also*, Decision 11-07-056, dated July 28, 2011, in Rulemaking 08-12-009. In this decision, the CPUC excludes from its definition of personal information any information from which identifying information has been removed such that an individual, family, household, etc., cannot reasonably be identified or re-identified.

SDG&E's Smart Grid Deployment Plan (SGDP)

San Diego Gas & Electric's (SDG&E) vision for its Smart Grid transformation is to work in collaboration with key stakeholders to create the foundation for an innovative, connected and sustainable energy future. Its deployment baseline is supported by a nearly complete smart meter rollout and Supervisory Control and Data Acquisition (SCADA)[15] coverage of roughly 80 per cent of its distribution system, among other existing systems and capabilities. SDG&E's Smart Grid deployment strategy prioritizes projects according to customer value, policy drivers and the need to pilot.

SDG&E's SGDP is not static but will evolve as the company's engagement with stakeholders continues in order to align its Smart Grid strategy to stakeholder priorities. The utility also plans to update its roadmap as customers, stakeholders, available technologies, and services evolve; adopt new security strategies as new threats or other risk conditions emerge; and adjust its cost/benefit estimates as its pilot and deployment experiences and new information bring greater certainty to anticipated inputs, timelines and outcomes.

An integral part of SDG&E's SGDP is its approach to privacy and security. SDG&E includes reference to several guiding principles related to customer privacy including the Fair Information Practice Principles (FIPPs) as detailed by the Federal Trade Commission, the National Institute of Standards and Technology's (NIST) four dimensions of privacy, as well as the seven *Privacy by Design* foundational principles as guidance for its privacy program. With this approach, privacy and security will be embedded at the earliest stages of system decision-making and will thus become incorporated into all aspects of design.

15 Supervisory Control and Data Acquisition. This system allows for short latency data acquisition and switching in the electrical grid of the utility.

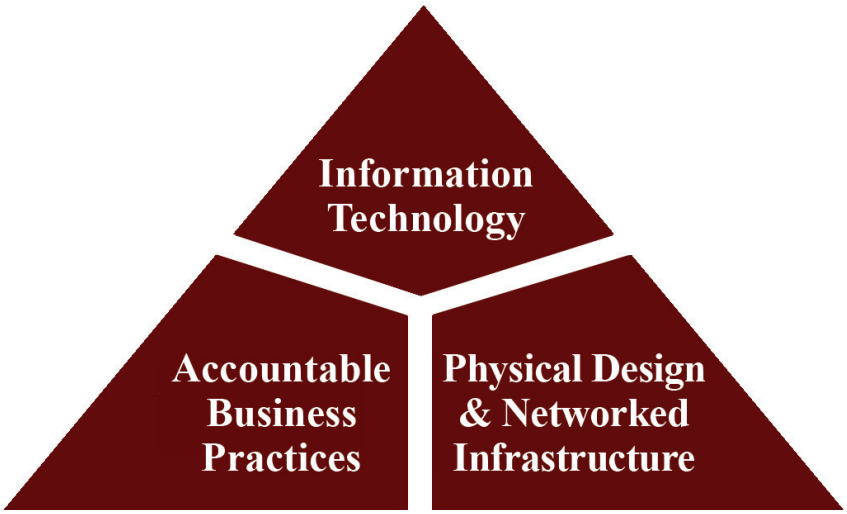
Privacy by Design

Privacy by Design (*PbD*) principles may be integrated right from the start as utilities begin their Smart Grid implementations, thus helping to make sure that customer information is protected. Embracing a positive-sum model whereby privacy, security and energy conservation may be achieved in unison is key to ensuring consumer confidence in electricity providers as Smart Grid projects are initiated. In addition, customer satisfaction with and trust of Smart Grid initiatives is an integral factor in the success of energy conservation and other goals of Smart Grid efforts.

The 7 Foundational Principles of Privacy by Design[16] incorporates the universal principles of the Fair Information Practice Principles (FIPPs). It represents an evolution from traditional approaches to protecting privacy, which focus on setting standards for information management practices, and providing remedies for privacy breaches, many of which come into play after the fact. By contrast, *PbD* is a proactive approach to privacy protection. It seeks to avoid data breaches and their consequential harm, thereby being preventative in nature.

These information management principles – and the philosophy and methodology they express – can apply to specific technologies, business operations, physical architectures and networked infrastructure – entire information ecosystems. FIPPs are affirmed by *PbD* principles, but *PbD* seeks to raise the bar in the area of privacy protection. Compliance with the CPUC rules which adopt the FIPPs fits well with, and is complementary to, *PbD* principles, which encourage a holistic view of privacy protection rather than a narrow focus on compliance with rules and legislation.

PbD is a concept developed by Commissioner Ann Cavoukian in the 1990s to address the ever-growing and systemic effects of information and communication technologies, and of large-scale networked data systems. *PbD* extends to a "trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.



16 See *The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*, available online at www.ipc.on.ca.

The objectives of *Privacy by Design* may be accomplished by practicing the 7 Foundational Principles of *Privacy by Design*:

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*

This approach, with its emphasis on positive-sum, win-win outcomes, continues to attract attention and gain support from around the world.[17] *Privacy by Design* was unanimously passed as an International Resolution by the global assembly of Privacy Commissioners and Data Protection Regulators in Jerusalem, in 2010.

17 See for example: European Commission, *Proposal for a General Data Protection Regulation*, COM(2012) 11 final, Article 30(3); European Commission Task Force Smart Grids, Expert Group 2 Report *Regulatory Recommendations for Data Safety, Data Handling and Data Protection Report* (16 February 2011), p. 16; and, Resolution, 32nd International Conference of Data Protection and Privacy Commissioners, *Privacy by Design Resolution*, 27-29 October 2010, Jerusalem, Israel.

SDG&E's Privacy Governance Framework

SDG&E's Customer Privacy Program

In the last 30 years the Internet has impacted privacy in ways that very few could have predicted. The Smart Grid looks to be another set of paradigm-changing technologies that will also change the way we look at consumer energy use data. As San Diego Gas & Electric (SDG&E) embarks on its efforts to implement its Smart Grid Deployment Plan (SGDP), it will be collecting more information than before about its customers. We must ask ourselves this question: How will Smart Grid deployments impact the privacy of utility customers and how will we manage this challenge?

SDG&E believes privacy is a fundamental right of every customer. It is committed to doing its part to advocate for privacy on behalf of its customers and its community. It works collaboratively with external partners to find ways to advance its privacy program.

SDG&E acts as a conscientious steward of customer information and their customers clearly expect that SDG&E is doing everything in its power to reasonably protect their privacy. SDG&E recognizes that customer information is required in order to provide safe, reliable service to the communities it serves and that this service requires SDG&E to responsibly collect, store, share and properly dispose of customer data when it is no longer needed. Without customer confidence in its ability to attend to these responsibilities, SDG&E cannot fully realize its business goals.

Therefore, one of the fundamental goals of SDG&E's privacy program is to continually earn the confidence of its customers by:

- building a strong culture of privacy within SDG&E;
- safeguarding the information customers have entrusted to them;
- adhering to fundamental privacy principles such as *PbD*, that put customer privacy first;
- complying with all applicable privacy laws and regulations and;
- last but not least, by listening to our customers' ideas and concerns about privacy and addressing them proactively.

Through the integration of *PbD* into its business operations, SDG&E intends to develop a fresh perspective on ways to improve its ability to protect the privacy of its customers.

Enterprise Information Risk Management

The framework SDG&E is implementing for the governance and oversight of its privacy programs within the company is founded on the belief that privacy is a fundamental right of every customer. *Privacy by Design* is being incorporated into the framework, which will comprise robust business rules as well as effective controls to protect the privacy of customer data. SDG&E is taking steps to integrate customer privacy within the business culture at SDG&E by raising awareness of privacy issues, and educating employees and contractors about the need to respect and protect customer

privacy. Privacy is also being embedded into company artefacts pertaining to projects and processes involving customer data, such as: company policies, guidelines, processes, procedures, security requirements, architectural principles and design standards, as well as system configurations. Business practices will be reviewed to ensure that the collection of customer information is minimized or eliminated, and that customer information is only shared with those who have a need to know the information. As much as possible, SDG&E will seek to automate data loss prevention initiatives to minimize the risk that sensitive information could be intentionally or accidentally mishandled.

In keeping with *Privacy by Design*, the protection of customer information is a core value and feature of SDG&E's Enterprise Information Risk Management (EIRM) framework. The EIRM is an ongoing process to proactively manage risk related to information. The objectives of the framework are to provide the company with a standard framework for managing information risk; provide the ability for the business to make informed information risk decisions; make the company aware of the potential risk impact to its information; and, continually assess, measure and improve processes. The EIRM proceeds by following four steps: Profile, Assess, Take Action, and Monitor.

Profile: Identifies company information.

Assess: Provides threat classification and security vulnerability information, along with potential business impact, to suggest possible responses to different categories of information risk.

Take Action: Empower business managers to make informed decisions to prioritize risks and implement appropriate controls.

Monitor: Ensures that current and future risks can be minimized through ongoing maintenance and monitoring activities.

Chief Customer Privacy Officer

SDG&E has a Chief Customer Privacy Officer as well as a working group that oversees privacy compliance. SDG&E's Chief Customer Privacy Officer is also the Vice-President of Customer Services and serves as a member of the Executive Management Team. Reporting to the Chief Customer Privacy Officer is a cross-functional, cross-departmental privacy team chartered to manage privacy matters for SDG&E. The Privacy Team has several areas represented including but not limited to: Billing, Commercial/Industrial Services, Credit, Customer Communications, Customer Contact Center, Customer Programs, Information Security, Legal, Load Management and Smart Grid.

The Chief Customer Privacy Officer's role is to ensure the completion of privacy impact assessments and other ongoing efforts, including influencing plans for the *Grid and Cyber Security Strategy* portion of the SGDP, and ensuring a robust approach to enterprise architecture, information modeling and standards with privacy. This includes plans for incorporating interoperability standards based on guidance from the National Institute of Standards and Technology, and the 7 Foundational Principles of *Privacy by Design*.

Organizationally, SDG&E's information security program is managed from its Information Technology division. As an emerging set of new capabilities, customer privacy is owned by the Chief Customer Privacy Officer and Vice President of Customer Services. This model allows SDG&E to place emphasis on privacy as a business-driven initiative which is essential to meeting privacy objectives, customer expectations and regulatory requirements in a timely fashion. Privacy and security share a strong relationship — robust privacy cannot be achieved without good information security. However, we must be careful not to treat them as one and the same.

For example, when considering a customer record from an information security perspective, SDG&E considers the level of protection the information requires and ensures controls are in place to protect its confidentiality, integrity and availability. In addition to those concerns, the privacy perspective must also consider whether the information needs to be collected at all, and if so, how its continued collection and use will provide value to the business and its customers. Privacy takes on a more customer-centric perspective, enabling features such as company transparency regarding the use of customer data, the ability to opt in to third party sharing, as well as other capabilities that conscientious customers consider important to managing their privacy but go beyond the scope of purely safeguarding their data.

Engineering of Products

During the Project Preparation phase, project teams identify the types of information that a product will handle, the custodians of that information, the sensitivity of the information, and the environments in which the information will be handled and accessed. At the Requirements phase review, the Preliminary Risk Assessment is reviewed along with the Requirements documentation to verify that the recommended controls are required as part of the project. At the Design phase review, the Design document is examined to identify if the design appears to effectively implement the required controls, and to identify any risk conditions or deficient controls that may not have been previously apparent. During the Build phase, the assigned Engineer provides direct support for implementation of controls by the project teams. In addition, the assigned Engineer performs some preliminary testing on baseline configurations of products, usually before customization and integration. At the Test phase, the product is tested for compliance with technical and administrative controls.

Roles and Responsibilities

Restricting the ability to access customer data on a strict need-to-know basis is another example of incorporating *Privacy by Design* at SDG&E. This will be done by way of technological features and controls to protect information from misuse, unauthorized access, unauthorized acquisition, destruction or disclosure. Limiting access will be based on business considerations and an individual employee's particular role at SDG&E.

To assist in implementing its need-to-know policy, SDG&E categorizes employees into five basic role types:

- **User:** An individual who accesses or attempts to access company information and/or Information Systems.

- Risk Owner: Company officer or executive that is ultimately accountable for risk and has the ability to assume financial impact of an accepted risk or the residual risk related to the outcome of a risk treatment.
- Risk Manager: Company executive or director who has been delegated a limited level of responsibility for making risk decisions on behalf of the Risk Owner.
- Control Owner: Directors or managers ultimately accountable for security controls. Control Owners report to Risk Managers any deficiency of controls related to the protection of company information and information systems. Control Owners don't necessarily need to organizationally report directly to a Risk Manager.
- Control Manager: Individuals responsible for implementing and maintaining operational controls. A secondary responsibility exists to ensure controls are operating effectively and performing as expected. Control Managers are assigned by and report deficiencies to Control Owners.

Vendor and Service Provider Contracts

Key privacy and security features are embedded into contracts with vendors and service providers. The general contract areas listed below are augmented with specific requirements based on the specific product or service addressed by the agreement. The contract language requires verifiable accomplishment of privacy and security goals and adherence to security standards and best practices; such verification may be performed by the company or a trusted third party. Contract language is intended to instil in third parties a necessary sense of urgency in protecting customer privacy. It describes third party obligations to protect information in alignment with industry accepted oversight and audit procedures. It further describes third party liability if they are the cause of a privacy breach.

Vendor and service provider contracts have specific language regarding:

- Role Based Security Controls;
- Shared Application Architecture;
- Account Management;
- Application Interface Controls;
- Encryption;
- Password and Logon Standards;
- Data Security;
- Logging and Errors Details;
- Operational Support and Administration;
- Source Code Review;
- Vulnerabilities and Defects;
- Security Assessments and Testing;
- Right to Report.

SDG&E's Smart Pricing Program

San Diego Gas & Electric (SDG&E) is nearing completion of its smart meter installations and the next step is to leverage the capabilities of these meters to a greater degree. As part of SDG&E's Smart Pricing Program, SDG&E will offer new pricing plans (i.e. time-variant rates) for residential and business customers beginning in 2013.[18] Providing customers choices in their energy decisions is a key driver of SDG&E's Smart Pricing Program, as well as helping customers to make more informed decisions based on their energy use consumption. The pricing options will allow customers to select a plan that best meets their needs and will provide them with an opportunity to save money. Over the long term, adoption of the new pricing plans is expected to help reduce greenhouse gas emissions by shifting energy use to time periods when more efficient and cleaner power plants are being used – all of which will benefit customers, communities and the environment.

Customers will use an energy management tool as part of the Smart Pricing Program to engage frequently with energy information so as to better understand when and how they use energy. The energy management tool will have the following features:

- Energy Use Analysis:
  Information provides insights into how the home or business uses energy;
- High-Bill Analyzer:
  A self-serve approach to understanding the changes in one's energy bill;
- Self-Audit:
  An assessment of a home's energy use with a customized energy saving plan;
- Goals & Alerts:
  Create personalized energy savings goals and sign up for goal-progress, high-bill, and event day reminders;
- Comparison & Selection:
  A quick and easy way to compare pricing options and select the plan that best meets one's needs.

Additional tools in support of the Smart Pricing Program include enhancements to existing systems to automate a number of features, including the determination of a customer's eligibility for the new pricing options, as well as customer notifications to reduce energy usage. The energy management tool will also support the management of outreach and education efforts.

To increase awareness and understanding about the new tools and pricing plans that will be offered as part of its Smart Pricing Program, SDG&E is undertaking significant outreach and education

18 Please refer to SDG&E Application (A.10-07-009): http://sdge.com/node/476 and General Rate Case (GRC) Phase II Application (A. 11-10-002) http://sdge.com/node/1527.

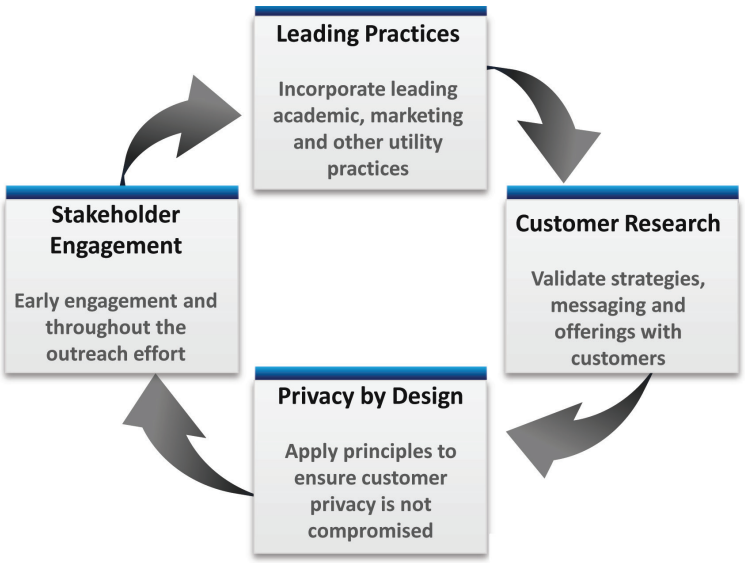
initiatives. SDG&E is committed to continuing its customer-centric approach as part of the Smart Pricing Program and has adopted five guiding principles to make sure that outreach and education efforts are developed and executed with this objective in mind. Foundational elements, including *Privacy by Design*, have informed SDG&E's education and outreach efforts (as depicted below).

In communicating with customers about smart pricing, SDG&E will focus on making the customer central in the delivery of services, while making it easy for customers to understand and exercise their own choices.

Customer Centric	**Deliver comprehensive service offerings that customers value**
Simplify	**Make it easy to understand, easy to do**
Listen	**Be collaborative, open and transparent**
Engage	**Motivate in an innovative and effective way**
Flexible	**Be willing to learn and adapt**

GUIDING PRINCIPLES

MARKETING ELEMENTS



Privacy by Design and the Smart Pricing Program

In setting privacy-related priorities for SDG&E, the Chief Customer Privacy Officer identified the Smart Pricing Program as a key area of *Privacy by Design* integration. The results of the integration will then be a model that can be replicated by other projects within SDG&E.

To kick off its efforts to implement *Privacy by Design* in the Smart Pricing Program, SDG&E met with the IPC in 2011 to better understand the concepts around *Privacy by Design* and the Smart Grid. SDG&E learned how the IPC worked with partners in the Ontario energy sector, including major utilities, to develop best practices for Smart Grid *Privacy by Design*[19] based on The 7 Foundational Principles of *PbD*:

1. Smart Grid systems should feature privacy principles in their overall project governance framework and proactively embed privacy requirements into their designs, in order to prevent privacy-invasive events from occurring.

2. Smart Grid systems must ensure that privacy is the default — the "no action required" mode of protecting one's privacy — its presence being assured.

3. Smart Grid systems must make privacy a core functionality in the design and architecture of Smart Grid systems and practices — an essential design feature.

4. Smart Grid systems must avoid any unnecessary trade-offs between privacy and legitimate objectives of Smart Grid projects.

5. Smart Grid systems must embed privacy end-to-end, throughout the entire life cycle of any personal information collected.

6. Smart Grid systems must be visible and transparent to consumers — engaging in accountable business practices — to ensure that new Smart Grid systems operate according to stated objectives.

7. Smart Grid systems must be designed with respect for consumer privacy, as a core foundational requirement.

To successfully achieve the objectives surrounding the Smart Pricing Program, SDG&E established a Project Management Office (PMO) dedicated to the implementation of the Smart Pricing Program as part of its Customer Services Division, under the leadership of the Chief Customer Privacy Officer. At the project level, a privacy team and privacy champions were established as essential organizational components to integrate privacy best practices. The following roles and responsibilities were established:

19 The full *PbD* Smart Grid Best Practices are contained in *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid* available online at www.ipc.on.ca

Privacy Team	• Interpret company privacy governance and apply same to project; • Handle project-specific privacy challenges and escalate to company privacy leadership as needed; • Be accountable for making sure project privacy deliverables are met and any risks are communicated to privacy leadership (CPO).
Privacy Champions	• Support project team members by acting as privacy subject matter experts; • Promote customer privacy, participate in training and awareness activities, and communicate relevant information; • May be responsible for specific project privacy deliverables.
Project Team	• Be fully aware of privacy principles; • Be capable of implementing privacy principles, and raising any issues/concerns with the Privacy Team and Champions.

Following their meeting with the IPC, the PMO asked its core privacy team to document these and further areas for *PbD* integration and key project deliverables. Based on the *PbD* principles for Smart Grid *Privacy by Design*, the team identified several options to integrate *Privacy by Design* into core project artefacts and business processes under each of the Best Practice headings.

1. Smart Grid systems should feature privacy principles in their overall project governance framework and proactively embed privacy requirements into their designs, in order to prevent privacy-invasive events from occurring:

Areas for Integration	Options
• Project Vision • Program Governance Plan • Product Life Cycle	➢ Develop Corporate Privacy Policy; ➢ Establish SDG&E Privacy Team; ➢ Identify DPP Privacy Team and Champions; ➢ Broadly communicate across SDG&E, DPP privacy objectives; ➢ Develop Privacy Impact Assessment Template.

Under this best practice, SDG&E's goal is to ensure that project team members make privacy a priority for the Smart Pricing Program by including privacy guidelines into the Project Governance Plan. A privacy team was established and privacy champions identified. A project-wide communication plan on privacy objectives was drafted and implemented. A privacy impact assessment template will soon be developed.

The project team began its initial Phase I development of IT requirements and construction, which was the ideal time to incorporate *Privacy by Design* into the beginning stages and foundation of the Smart Pricing Program. As a first step, the team identified the need to incorporate privacy controls and checkpoints into the IT Product Life Cycle, at each of the concept, business case, requirements, and design phases. The team will also set aside standard privacy controls and requirements into a central repository so that any project team member can pull the privacy requirements and use them for system testing. This will ensure that privacy requirements and system design pass system testing, and any defects are identified and resolved. A comprehensive business requirements privacy checklist was completed to determine the potential scope of personal information collection required by the Smart Pricing Program.

More importantly, there is also the commitment to document and review the means by which to measure success. The project team has committed to measuring its success and has identified for itself critical success factors such as: a) enhanced employee awareness of privacy; b) improving customer understanding and satisfaction with the Smart Pricing Program's approach to privacy and most importantly: c) limited exposure to privacy incidences.

2. *Smart Grid systems must ensure that privacy is the default — the "no action required" mode of protecting one's privacy — its presence is assured:*

Areas for Integration	Options
• Policy Framework • Requirements • Data Collection Processes • Data Sharing Processes	➢ Establish "opt-in" as default privacy setting requirement; ➢ Develop Q&A checklist for privacy default considerations for each phase of the project (development of business requirements, design, construct).

Applications within the Smart Pricing Program are being examined to ensure that they collect only the minimum information required to provide safe and reliable service. Any additional information should require users to act and positively consent (i.e., opt-in) to share more information. Users should be able to select the amount of information they wish to share, and it should not be all or nothing. As such, the opt-in default setting was established as a privacy goal within the Smart Pricing Program. Checklists are being developed so that measures to protect privacy are integrated into the full range of requirements, design and testing.

3. Smart Grid systems must make privacy a core functionality in the design and architecture of Smart Grid systems and practices — an essential design feature:

Areas for Integration	Options
• Business Use Cases • Business Requirements • System and Process Design	➢ Privacy viewpoint; ➢ Privacy principles; ➢ Privacy Q&A checklist; ➢ Include Privacy Controls in Security Requirements; ➢ Include Privacy in Request for Proposal.

The project team considered how to ensure user privacy right from the beginning of the project by clearly spelling out privacy requirements and giving them a high priority. The mechanisms identified to make privacy an essential design feature were an Enterprise Architecture Privacy Viewpoint, Enterprise Architecture Privacy Principles, Privacy Quality Assurance Checklist, and Draft of Privacy Controls in Security Requirements. Privacy is a required feature in all requests for proposal to develop technologies associated with the Project.

An important consideration is to have all third party contracts include customer privacy provisions. As such, developing a contract for the energy management tool involved considering several options to ensure that privacy would be a required component of the tool. Clauses regarding data minimization, etc., will serve to ensure that the final product is designed with privacy embedded as the default. A requirement was included in the energy management tool vendor contract to collect, use and disclose only the minimum amount of customer information necessary to ensure that system quality and the range of services would not be diminished for the energy management tool.

4. Smart Grid systems must avoid any unnecessary trade-offs between privacy and legitimate objectives of Smart Grid projects:

Areas for Integration	Options
• Culture • Awareness & Training • Decision Making • Project Planning	➢ Communications plan includes awareness for DPP team members; ➢ Reconsider options when a perceived trade-off may occur.

The project team developed a process and communication plan to raise awareness within the team to reconsider options when a perceived privacy trade-off may occur. Within this process, decision-makers refer to privacy requirements when potential trade-offs arise, and the project team determines how to enable services while meeting all privacy requirements.

5. Smart Grid systems must build in privacy end-to-end, throughout the entire life cycle of any personal information collected:

Areas for Integration	Options
• Security Requirements • Design • Testing • Information Management Life Cycle • Third Party Contracts • Auditing • Records Retention & Destruction	➢ Privacy Q&A Checklist is reviewed by Privacy Team at agreed upon points in the life cycle; ➢ Privacy is included in test strategy/plan; ➢ Security requirements are reviewed & updated to align with privacy requirements; ➢ Documenting/escalating privacy concerns and creating change orders to resolve any issues.

Privacy controls will be included in the master test plan. The Privacy Quality Assurance Checklist shall be included and reviewed by the privacy team at agreed upon points in the information life cycle to ensure that the project team meets all privacy and security requirements. In doing so, the project team will capture and secure information flow from the time of collection until it is securely destroyed, according to records retention requirements.

6. Smart Grid systems must be visible and transparent to consumers — engaging in accountable business practices — to ensure that new Smart Grid systems operate according to stated objectives:

Areas for Integration	Options
• User Presentation at time of Data Collection • User Presentation Self-help • Marketing Plan • Auditing of the process during its life cycle	➢ Privacy language, references and FAQ are available in customer-facing interfaces; ➢ Call Center is provided appropriate materials to answer privacy questions; ➢ Marketing Strategy and Plan include privacy objectives; ➢ Independent audit of privacy controls.

The project team's goal is to have users understand how the company protects customers' privacy by addressing privacy objectives in its Customer Outreach and Education plan. Users should know exactly why an application collects data about them and what their options are, and know what to do if they believe SDG&E is failing to meet their privacy expectations. In return, the company responds quickly and respectfully to user privacy concerns. Privacy language, references and FAQs should be available in customer-facing interfaces, and Call Centers will receive appropriate materials for answering privacy questions regarding the Smart Pricing Program. In accordance with attachment D to CPUC Decision 11-07-056, a notice titled "Notice of Accessing, Collecting, Storing, Using and Disclosing Energy Usage Information," has been developed and will be provided to new customers upon account activation and a link to this notice provided to all customers on an annual basis.

7. Smart Grid systems must be designed with respect for user privacy, as a core foundational requirement:

Areas for Integration	Options
• Culture • Awareness & Training • Functional Requirements • Contractors • Staff Performance Reviews	➢ Marketing Strategy contains privacy goals; ➢ Test Strategy includes privacy; ➢ Deliver brief privacy training to project team; ➢ Incorporate user perspective into service agreements and specifications.

Every employee that touches or produces Smart Pricing Program artefacts must understand the need to protect customer privacy and treat it with urgency. To realize this, Call Center staff will receive appropriate materials to respond to customer privacy questions about SDG&E's home energy management tool. The project team actively seeks to make privacy a priority for the project, and privacy training is delivered to all project team members. In addition, the project team will incorporate user perspectives into service agreements and specifications.

Conclusion

Applying new technologies to the existing electrical infrastructure in an effort to create a Smart Grid is a paradigm-changing process that will culminate in a revolution in the energy industry. However, with great change, there can also be numerous unforeseen consequences. For the Smart Grid, the challenge will be to recall the societal values we hold to be imperative, such as the fundamental right of privacy, and ensure their continuation in future architecture and business practices surrounding the provision, delivery and use of electricity.

These new technologies, from smart meters to in-home devices, are imperative to bring about Smart Grid enhancements, such as SDG&E's Smart Pricing Program. Nevertheless, these same technologies will make accessible some of the most sensitive data available about individuals – their patterns of behavior within the home. SDG&E recognizes and is planning for the protection of its customers' privacy, not only because customers expect it, but because SDG&E shares the view that privacy is a fundamental human right in a free and democratic society.

As this paper has shown, when adopting the approach of *Privacy by Design*, the value of privacy permeates all aspects of project planning from the project governance framework, to each stage of building and testing of the systems involved. Privacy incorporated in this way naturally leads to customer satisfaction, employee awareness, and system functionality. By taking a leadership position in using *PbD*, SDG&E places itself at the center of California's impressive track record in the protection of privacy and in advancing the Smart Grid.

From here, as SDG&E moves forward with its SGDP, which includes *PbD*, the Information and Privacy Commissioner of Ontario, Canada and SDG&E hope that our documentation of these approaches will help many more utilities and third party service providers in striving to preserve and place at the center their energy, consumers' privacy. Realizing that the vision of the Smart Grid will depend greatly on the participation of consumers who wish to be informed and empowered about their privacy, SDG&E is acting upon that vision.

Overview of Organizations

Information and Privacy Commissioner of Ontario, Canada

The role of the Information and Privacy Commissioner of Ontario, Canada is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The IPC acts independently of government to uphold and promote open government and the protection of personal privacy. Under the three *Acts*, the Information and Privacy Commissioner: resolves access to information appeals and complaints when government or health-care practitioners and organizations refuse to grant requests for access or correction; investigates complaints with respect to personal information held by government or health-care practitioners and organizations; conducts research into access and privacy issues; comments on proposed government legislation and programs; and educates the public about Ontario's access and privacy laws.

San Diego Gas & Electric (SDG&E)

SDG&E is a regulated public utility that provides safe and reliable energy service to 3.4 million consumers through 1.4 million electric meters and 855,000 natural gas meters in San Diego and southern Orange counties. The utility's area spans 4,100 square miles. SDG&E is a subsidiary of Sempra Energy (NYSE: SRE). Sempra Energy, based in San Diego, is a Fortune 500 energy services holding company with 2010 revenues of US$9 billion. The Sempra Energy companies' 17,500 employees serve more than 31 million consumers worldwide. In collaboration with other agencies, organizations and community leaders, SDG&E is creating a foundation for an innovative, connected and sustainable energy future. Our vision for a Smart Grid future is driven by both public policies and our customers who are adopting technologies like rooftop solar and electric vehicles at rates higher than anywhere else in the nation. Our ten-year Smart Grid Deployment Plan includes our vision for the future as well as the strategy and road map for achieving that vision.

Appendix A – California Public Utility Commission Decision 11-07-056

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

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

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

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

[T]he "*Privacy by Design*" methodology offers a promising approach to ensuring that data practices promote privacy, not just in the FIP of data minimization, but in all aspects of privacy planning…

** excerpts **

Appendix B - SB17

Chapter 4. Smart Grid Systems

8360. It is the policy of the state to modernize the state's electrical transmission and distribution system to maintain safe, reliable, efficient, and secure electrical service, with infrastructure that can meet future growth in demand and achieve all of the following, which together characterize a smart grid:

(a) Increased use of cost-effective digital information and control technology to improve reliability, security, and efficiency of the electric grid.

(b) Dynamic optimization of grid operations and resources, including appropriate consideration for asset management and utilization of related grid operations and resources, with cost-effective full cyber security.

(c) Deployment and integration of cost-effective distributed resources and generation, including renewable resources.

(d) Development and incorporation of cost-effective demand response, demand-side resources, and energy-efficient resources.

(e) Deployment of cost-effective smart technologies, including real time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices for metering, communications concerning grid operations and status, and distribution automation.

(f) Integration of cost-effective smart appliances and consumer devices.

(g) Deployment and integration of cost-effective advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal-storage air-conditioning.

(h) Provide consumers with timely information and control options.

(i) Develop standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid.

(j) Identification and lowering of unreasonable or unnecessary barriers to adoption of smart grid technologies, practices, and services.

** excerpt **

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: (416) 326-3333
Fax: (416) 325-9195
Email: info@ipc.on.ca

San Diego Gas & Electric®
P.O. Box 129831
San Diego, CA 92112-9831
Telephone: 1-800-411-7343
Email: info@sdge.com

March 2012

Privacy by Design: www.privacybydesign.ca

SDGE connected
A Sempra Energy utility™

Information and Privacy Commissioner, Ontario, Canada