Privacy by Design and Third Party Access to Customer Energy Usage Data

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

Jules Polonetsky
Co-Chair, Future of Privacy Forum

Foreword by Caroline Winn
Vice President, Customer Services,
Chief Customer Privacy Officer,
San Diego Gas & Electric (SDG&E)

January 2013

SDGE connected
A Sempra Energy utility™

Information and
Privacy Commissioner,
Ontario, Canada

THE FUTURE OF PRIVACY FORUM
WWW.FUTUREOFPRIVACY.ORG

Acknowledgements

The authors wish to acknowledge the research and writing contributions of Michelle Chibba, Director of Policy and Special Projects, IPC, and Policy Department staff, as well as Future of Privacy Forum staff Andrew Clearwater. We are also grateful to Caroline Winn, Vice President and Chief Customer Privacy Officer of SDG&E, and her staff, Christopher Vera, Manager of the SDG&E's Office of Customer Privacy, and Brendan Blockowicz, Technology Strategy Manager, for contributing to this paper SDG&E's experience with implementing Green Button.

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

TABLE OF CONTENTS

Foreword

It's hard to believe it has already been a full year since I worked with Dr. Cavoukian and her team on our paper, *Applying Privacy by Design Best Practices to SDG&E's Smart Pricing Program*. Since then, our respective Offices have continued to work hard on privacy in the Smart Grid world, engaging with many stakeholders around the world. At SDG&E, we have worked collaboratively with our 3.4 million customers, placing their privacy first and ensuring that we continue to be good custodians of their data within our privacy program. SDG&E was proud to be named the most intelligent utility in the U.S. by Intelligent Utility, for three years in a row!

When we published that first paper, our intention was to raise awareness and highlight privacy as an issue in the development of Smart Grid infrastructure and projects, and to highlight how elements of *Privacy by Design* were being considered in SDG&E's Smart Pricing Program. Throughout, it has been important to clarify that ***customer energy privacy***, that is, privacy around the collection and use of a customer's usage data, has become as an important part of the privacy discussion as a customer's personal information, and thankfully, this is now widely acknowledged and understood in North America and beyond. However, this area is moving very fast and there is increasing discussion about the use of consumption information. The data that is collected over the Smart Grid, stored on it, or transmitted by it is an incredibly important asset with the potential to benefit not only the customer and their utility, but also third parties, including research institutions, government organizations and other entities that seek to participate in some way on the Smart Grid. I applaud Dr. Cavoukian and Jules Polonetsky for taking a leadership role and addressing this issue by examining third party access to usage information (referred to in this paper as CEUD, or customer energy usage data), its potential benefits, and how *Privacy by Design* can ensure that privacy is protected in those scenarios. For the purposes of this new paper, I am pleased to offer an overview of SDG&E's experience in this area, specifically with regard to our implementation of the Green Button initiative.

There are sound reasons why energy consumers should remain in control of the energy consumption information they produce, even if the law does not require it. This is because the underlying benefits of Smart Grid, including energy conservation and customer choice, are negated without strong consumer confidence and trust in the Smart Grid and how customer energy privacy is respected. Gaining and retaining the trust of our customers is vital if we are to achieve the vision of a robust Smart Grid.

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

Introduction

The increased availability of customer energy usage data (CEUD) is one of the numerous benefits of Smart Grid improvements.[1] CEUD allows for more efficient power use by utilities and customers to better deal with spikes in demand. Utilities can avoid having to use expensive "peaker plants" which kick in when energy demands exceed normal levels of supply. And with greater access to information about their own CEUD, customers can make more informed choices about when and how much electricity to use.[2]

In an electrical grid designed primarily to deliver electricity from point 'A' to point 'B', there would be little use for, or concern regarding, third party access to CEUD. However, efforts to create a Smart Grid involve making infrastructure improvements enabling a bi-directional flow of information. As a result, smart meters and communication systems that help utilities meet Smart Grid objectives will end up collecting detailed information on individual energy consumption usage and patterns within homes. With this information, utilities have the ability to manage complex demands. Conversely, changes to the electrical grid inevitably make the privacy of CEUD a front-burner issue, and in particular, as it relates to third party access to CEUD. While this paper deals with third party access to CEUD, our focus is less on third parties that have traditionally assisted utilities with services such as billing, etc. We focus here on a new class of third parties wishing to gain access to granular and customer-specific CEUD (e.g. app developers, software vendors, device manufacturers, consumer service providers, and home security companies, etc.).

Privacy concerns and risks which arise from the detailed collection of personal information by utilities participating in a Smart Grid have been extensively covered by the Information and Privacy Commissioner of Ontario (IPC) in several papers (see the Appendix). In those papers, we apply the concept of *Privacy by Design* (*PbD*) to demonstrate that the benefits of the Smart Grid may be achieved while at the same time also protecting privacy. We acknowledge there are a number of jurisdictions with existing and developing regulatory requirements concerning this issue. This paper is not meant to apply to a particular jurisdiction, nor is it meant to be prescriptive. In this paper the IPC and the Future of Privacy Forum (FPF) explore at a high level the issue of third party access to CEUD, the benefits of such access, as well as the potential privacy risks. *PbD* will be described and examples of proactive approaches to privacy already underway, in the context of third party access to CEUD, will be detailed.

1 Smart Grid objectives include energy efficiency, incorporating alternative energy sources, increased consumer choice, and robust cyber security.

2 For example, a smart thermostat that is able to get rate data is able to be smarter and save more money. The smart thermostat is able convert access to energy data into a consumer benefit and it does this in a way that is transparent to the consumer but is still simple to use. Devices such as refrigerators, thermostats, and washers/dryers can be improved to save money on energy consumption. The results of this communication are even more striking when smart appliances are able to respond to variable pricing to avoid usage during peak rates when demand for electricity is high.

Opportunities for innovation in allowing access to CEUD

Advocates for innovation argue that allowing third parties access to CEUD will lead to new products and services that will support conservation and unleash more innovations. The Obama administration's "Energy Data Initiative," for example, encourages entrepreneurs to use energy data to develop tools for energy consumers.[3] Led by the U.S. Department of Energy, the initiative provides grant-funding opportunities, and has held an "Apps for Energy" (or "Datapalooza") contest[4] in which the people's choice award for best energy app went to an Ontario-based company called Zerofootprint for their app VELObill.[5] If proper privacy practices are employed, new innovations such as VELObill can provide a great opportunity for consumers and for third party companies that seek to serve them.

Privacy as an issue in the context of innovation opportunities in third party access to CEUD is specifically being examined by the MaRS Discovery District,[6] an innovation center based in Toronto, Canada, that has worked closely with companies such as Zerofootprint. MaRS launched a Data Catalyst project which aims to get CEUD into the hands of innovators in a secure, privacy-protective and usable way, to drive energy conservation and spur economic growth.[7] In a recently issued report,[8] MaRS stated that by placing the choice to access and use data securely in consumers' control, or by including no personal information, "smart disclosure"[9] can successfully incorporate privacy within third party access to CEUD.

	Consumer	Commercial		Industrial
New applications and solutions	Consumer and smart home applications drive behavior change and conservation	Employee engagement and process improvements drive conservation	District energy balances large nearby consumers, particularly peak loads	Data analytics for business optimization and customer segmentation
Value of the user market	Utility bill savings generate consumer surplus	Reduction in variable energy costs gives savings to businesses	Reduction in fixed and peak contracts gives cost savings to businesses	Cost reduction to utility companies and grid operator
Value of the supplying market	Application development, hardware and telecoms revenue and job creation	Application development and advisory services revenue and job creation	Professional services and advanced building monitoring systems revenue and job creation	Software and professional services revenue and job creation
Value to utility and grid operators	Revenue reduction balanced against lower generation and infrastructure costs	Revenue reduction balanced against lower generation and infrastructure costs	Revenue reduction balanced against lower generation and infrastructure costs	Cost reduction in key customer service, planning and asset management operations

Source: MaRS Data Catalyst, 2012

Figure 1 – Economic benefits of smarter use of CEUD

3 http://www.data.gov/communities/node/48/events/energydatainitiative

4 http://appsforenergy.challenge.gov/

5 http://appsforenergy.challenge.gov/submissions/7930-velobill-the-utility-bill-of-the-future

6 http://www.marsdd.com/

7 http://datacatalyst.marsdd.com/energy/

8 http://www.marsdd.com/news-insights/the-market-impact-of-accessible-energy-data/

9 The term "smart disclosure" refers to the timely release of data in standardized, machine-readable formats.

Leveraging the millions of dollars already invested in smart meter deployments and other Smart Grid improvements can lead to downstream market opportunities. At the end of 2011, there were more than 33 million U.S. energy customers with smart meters.[10] In Ontario, nearly every residential and small business customer has smart meters.[11] Between 2005 and 2011, Ontario's conservation efforts decreased electricity consumption by 1900 megawatts, which is comparable to taking 600,000 homes off the Ontario grid.[12] MaRS has identified the main business segments that can benefit from the unique electricity data assets and expertise arising in the area of access to CEUD, including:

- *Customer and small business applications:* electronic information displays to visualize energy consumption, home area networks that connect home appliances and other devices to a central connection point, smart appliances, and other solutions for remote engagement by the customer;
- *Building management and retrofit:* once a customer has identified an energy savings goal, there may be opportunities for building management and retrofit businesses to offer the appropriate products and services;
- *Commercial software for utilities:* software can better manage and analyze meter data for improved system performance, and to maximize business value of smart meter data. For example, utilities could analyze customer behaviour and create customer segments to offer better price plans and lower peak usage (win-win for consumer and utility).

10 http://www.eia.gov/todayinenergy/detail.cfm?id=8590

11 As of August 31, 2012 there were 4,777,720 installed smart meters, 4,461,702 meters enrolled with the MDM/R (6,450 added in August) and 4,391,679 customers on TOU billing (56,267 added in August). http://www.ontarioenergyboard.ca/OEB/_Documents/SMdeployment/Monthly_Monitoring_Report_August2012.pdf

12 http://www.metering.com/node/21846

Recognizing the privacy risks of providing access to CEUD

Although the definition of informational privacy will differ among jurisdictions, the essence of privacy relates to one's ability to exercise control and have freedom of choice relating to the collection, use and disclosure of information about oneself—one's personal data flows.[13] The initial privacy risk already explored in previous literature (see the Appendix) relates to how improvements to the electrical grid introduce new technologies that increase the granularity of information collected on household energy usage. The literature has explored and made recommendations about: increasingly sophisticated metering technologies; increased collection of energy consumption data; and the potential to glean intimate details about one's household activities. Beyond the concerns already identified, however, the consequence of third party access to CEUD is that it may allow entities other than utilities to use CEUD, and in entirely new ways.

While this area is still evolving, for the purposes of this paper, we identify the following basic data flow scenarios for third party access to CEUD:

Utility-to-customer	In this scenario, CEUD goes directly from the utility to the customer (e.g. Green Button "Download My Data"), and the customer could subsequently choose to forward his or her data to a third party. The third party must establish relationship with the customer independent of the utility, and there is no contractual relationship between the utility and the third party.
Utility-to-third party	*Customer authorization:* In this scenario, CEUD is transferred from the utility to a third party with the customer's authorization (e.g. Green Button "Connect My Data"). The third party must establish a relationship with the utility and the consumer, and there is no contractual relationship between the utility and the third party. *Primary purpose:* In this scenario, CEUD is transferred from the utility to a third party without the customer's consent for a "primary purpose." In this case, the third party must a establish relationship with the utility. There is a contractual relationship between the utility and the third party.
Device-to-customer	In this scenario, a device, such as a HAN-enabled device, installed at the customer's house obtains the CEUD from the smart meter and the consumer could subsequently choose to forward his or her data to a third party. The third party must establish relationship with the customer independent of the utility, and there is no contractual relationship between the utility and the third party.

13 It is important to distinguish personally identifiable from non-identifiable data on the Smart Grid. Smart meters, while a very important element of the Smart Grid, actually represent a small fraction of the overall grid. The vast majority of the Smart Grid has to do with the operation of the power network rather than pertaining to individual energy customers. Since the monitoring and control of the grid does not require the use of any personally identifiable information under normal operations, privacy concerns remain practically non-existent.

While a privacy impact assessment and threat risk assessment should be conducted regarding any new IT initiatives involving new collections, uses, and disclosures of personal information, including CEUD, the following are three high level areas in which privacy issues may arise within the context of third party access to CEUD:

Information technology	'Information technology' encompasses the development and use of computers, devices, networks and associated applications which can be used to protect and control access to personal information. This includes access controls, audit controls, data integrity, authentication, and the security of transmission and storage of personal information.
Accountable business practices	'Accountable business practices' refer to a business' actions, policies and procedures directed towards the collection, use and disclosure of personal information. These will be an organization's overall privacy management processes, responsibilities and evaluation, including workforce privacy awareness and training, access policies and management, as well as contracts and agreements.
Physical design and networked infrastructure	'Physical design and networked infrastructure' refers to the physical measures, policies and procedures that are aimed at protecting IT equipment and infrastructure, and securing the area they are located from unauthorized access. This includes controlling who has access to the facilities where equipment is located, as well as policies on the use of workstations, devices and other media.

Privacy issues may arise in any of these three areas, especially, for example, when a third party seeks to securely access CEUD from a utility's backhaul. In addition, the development of accountable business practices can impact privacy in varying degrees, such as the design of authorization methods, the definition of primary versus secondary uses of CEUD, and any clauses contained in contractual arrangements that ensure the third party follows accepted privacy practices. These risks should be approach proactively from a positive-sum and privacy-enabling perspective to reach the intertwining goals of encouraging innovation and privacy protection regarding third party access to CEUD.

Minimizing privacy risks with *Privacy by Design*

Taking a proactive approach lies at the heart of *Privacy by Design* ('PbD')[14] which involves embedding privacy directly into the design of technologies, business practices, and networked infrastructures. It makes privacy a foundational requirement, anticipating and preventing privacy-invasive events **before** they happen. *PbD* was developed back in the 1990s by Commissioner Ann Cavoukian, Ph.D., when the notion of embedding privacy into the design of technology was far less popular. At that time, taking a strong regulatory approach was the preferred course of action. With advanced digitization of data, networked infrastructure, social networking, etc., it is now clear that the future of privacy cannot be assured solely by compliance with regulatory frameworks.[15] Rather, privacy assurance must ideally become an organization's default mode of operation over three areas of application: (1) information technology; (2) accountable business practices; and (3) physical design and networked infrastructures.

Based on a set of 7 Foundational Principles, *PbD* offers a flexible and technology-neutral vehicle for engaging with privacy issues, and for resolving them in ways that support multiple outcomes in a positive-sum, win/win scenario as opposed to a zero-sum, either/or scenario. The Principles are as follows:[16]

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*

14 Cavoukian, Ann. "*Privacy by Design.*" Office of the Information & Privacy Commissioner of Ontario, 2009.

15 This perspective is acknowledged internationally. Privacy leaders from around the world have endorsed the importance of PbD. At the 32nd International Conference of Data Protection and Privacy Commissioners in 2010, PbD was unanimously passed and adopted as an International framework for protecting privacy. International Conference of Data Protection and Privacy Commissioners (2010). Privacy by Design Resolution, adopted at Jerusalem, Israel, October 27-29, 2010. At http://www.privacybydesign.ca/content/uploads/2010/11/pbd-resolution.pdf.

16 Information and Privacy Commissioner of Ontario. "*Privacy by Design*: The 7 Foundational Principles." (2009).

The aim of this proactive approach is to reduce the risk of privacy harm from arising in the first place, ideally preventing it entirely, while preserving a commitment to functionality. Privacy is often viewed as an individual right that must be sacrificed in order to attain other socially desirable, but perhaps competing goals. Privacy is often "traded off" to achieve other goals such as security, for example. However, it is the Commissioner's view that such zero-sum thinking must be changed to a doubly-enabling positive-sum paradigm, where both the need for privacy and the need for security may both be satisfied.

In 2011, a landmark resolution by the Information and Privacy Commissioner, Dr. Ann Cavoukian, was approved by International Data Protection Regulators and Privacy Commissioners in Jerusalem at their annual conference. The resolution recognizes the concept of *Privacy by Design* as an "essential component of fundamental privacy protection." It encourages the adoption of the principles of *Privacy by Design* as part of an organization's default mode of operation. The resolution also invites Data Protection Authorities and Privacy Commissioners to promote *Privacy by Design*, foster the incorporation of its 7 Foundational Principles into privacy policies and legislation in their respective jurisdictions, and encourage research into *Privacy by Design*.

The IPC has written extensively on the need to build privacy into Smart Grid projects, including guidelines and case studies which show the operationalization of *Privacy by Design* in the Smart Grid. For a complete list of all six papers, please see the Appendix.

Planning for privacy prior to accessing CEUD

Recent efforts to better understand and plan for the impacts on privacy of third party access to CEUD have begun to set parameters for third party access, while striving to promote customers' empowerment through control of their own energy usage data. Some examples of early thinking about privacy within the context of third party access to CEUD can be found in regulatory and industry-led approaches such as those put forward by the California Public Utilities Commission,[17] the North American Energy Standards Board,[18] and the National Institute of Standards and Technology.[19] Below, we detail additional examples of industry-led approaches to privacy issues in third party access to CEUD involving aggregated smart meter readings, a data de-identification tool, efforts at consumer education, a privacy seal initiative, and a customer access to CEUD initiative dubbed "Green Button."

Aggregated Smart Meter Readings

While there have been multiple technologies developed to embed privacy into the functioning of smart meters themselves, we will profile a protocol for the aggregation of smart meter readings developed by Klaus Kursawe, George Danezis, and Markulf Kohlweiss. These researchers deal with a critical privacy issue surrounding smart metering – the transmission of detailed electrical usage data to the utility or to third parties. Specifically, they note that rather than trying to separate personally identifiable data from the remaining data, it is best to determine what data is required to perform a task, and ensure that only that data is collected. Extending this line of reasoning, the researchers felt that (except for billing purposes and consumer awareness), a utility or third party may not need to access any individual consumption data – it may be sufficient to have aggregate consumption data for a particular area. To these ends, the researchers developed two smart meter data aggregation protocols:

- **"Diffie-Hellman"-based Private Aggregation (DiPA) protocol**: A homomorphic commitment scheme can allow a user (in this case, a smart meter) to "commit" to a secret, and later reveal the secret and prove that this was the value to which it committed. For smart meters, DiPA makes it possible to submit a commitment to an aggregate reading from multiple smart meters (the sum total of their energy usage), such that the end recipient gets the required verifiable demand management data, without knowing any information about individual household consumption.

- **Low Overhead Private Aggregation (LOPA) protocol**: Each pair of meters in an aggregation group shares a different secret value (that is, for an aggregation group of 10 meters, each meter holds nine shared secrets). When transmitting readings, one meter in the pair adds the secret value to its actual value, and

17 Decision 11-07-056, http://docs.cpuc.ca.gov/WORD_PDF/FINAL_DECISION/140369.pdf

18 NAESB REQ.22 http://www.naesb.org/retail_request.asp

19 http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

the other subtracts it (thus, in a group of 10 meters, each submitted reading has had nine secret values added to or subtracted from it).

The researchers implemented the DiPA and LOPA protocols on production meters from Elster SG. The computation overhead of the masking process was found to be far below one second, which does not create any latency issues even for frequent (every 15 minutes) readings of smart meters. For more information, see "Smart Meters in Europe: *Privacy by Design* at its Best" (available online, www.ipc.on.ca).

Data De-Identification Tool

In the vast majority of cases, de-identification will strongly protect the privacy of an individual's CEUD when additional safeguards are in place. The claim that de-identification has no value in protecting privacy due to the ease of re-identification is merely a myth. If proper de-identification techniques and re-identification risk management procedures are used, re-identification becomes an extremely difficult task.[20] Dr. Khaled El Emam[21] developed a strong de-identification tool that simultaneously maximizes privacy and data quality while minimizing distortion to the original database. Initially developed to de-identify health-related data, it minimizes the risk of re-identification for any data set based on:

- The low probability of re-identification;
- Whether mitigation controls are in place;
- Motives and capacity of the recipient;
- The extent a breach invades privacy.

Dr. El Emam was approached to create a longitudinal public use dataset using his de-identification tool for the purposes of a global data mining competition – the Heritage Health Prize. Participants in the Heritage Health Prize competition were asked to predict, using de-identified claims data, the number of days that patients would be hospitalized in a subsequent year. Before releasing the dataset created using Dr. El Emam's tool, the de-identified dataset was subjected to a strong re-identification attack by a highly skilled expert. The expert was not successful and concluded that the dataset could not be re-identified.

20 Cavoukian, A., & Emam, K. E. (2011). "Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy": Office of the Information & Privacy Commissioner of Ontario; and, El Emam, K., Jonker, E., Arbuckle, L., & Malin, B. (2011). "A systematic review of re-identification attacks on health data." PLoS One, 6(12), e28071.

21 Leading investigator at the Children's Hospital of Eastern Ontario Research Institute and Canada Research Chair in Electronic Health Information.

Transparency and Consumer Education

Xcel Energy, which provides power to consumers in eight western and midwestern states, is a good example of a utility implementing a privacy program for third party access to CEUD that incorporates transparency and consumer education. At its web site, Xcel provides consumers with detailed but easy to understand information about smart meters, including how they work, how data is collected and the choices that are available. Consumers are provided with the ability to view their own data in a variety of charts and tables that help them understand their energy usage.[22] Consumers are also provided with the necessary forms to enable transfer of their data to third parties and are provided with an extensive description of the data types that will be included when such data is transferred.

Visibility and Transparency are foundational *Privacy by Design* principles. Many utilities are focused on privacy as they deploy smart meters, but not all have provided easy to find and detailed privacy information publicly describing their CEUD related privacy practices at their Web sites. Xcel provides an example on how utilities can post privacy policies that include details about web site privacy information and the necessary information needed by consumers, regulators, and partners to understand how smart grid data is collected and used.[23]

Privacy Seal

"Privacy seals" are self-regulatory programs aimed at ensuring consumer privacy by way of independent third party enforcement of responsible data practices. The Future of Privacy Forum (FPF), working with key stakeholders, has created a self-regulatory seal program powered by independent third party enforcer, TRUSTe, to ensure that companies wishing to gain access to CEUD commit to responsible privacy practices. The seal provides privacy guidelines and support for utilities, regulators, and others who wish to ensure the development of policies that respect privacy, as well as for companies that access consumer energy or smart home data. The seal is available to companies offering home energy management, remote home control or security systems that seek to access CEUD.

To create the program, FPF and TRUSTe received input from utilities and utility regulators and companies including AT&T, Comcast, Ecofactor, IBM, Intel, Motorola, Neustar, OPower, Tendril, and Verizon. An advisory committee including Edison Electric Institute (EEI), the GridWise Alliance, and consumer advocates will also

22 Xcel Energy: Energy Consumption Data Access https://www.xcelenergy.com/My_Account/Understand_Bill/Bill_Details/Energy_Consumption_Data_Access (The report contains the following information: Customer name, Account number, Date report was created

Utility type: electricity or natural gas, Service number, Meter number, Address: street number, street, apartment number, city, state, ZIP code, Premises number, Premises description, Tariff description, Date meter was read, Number of days in billing period, Total usage, Average use per day (kWh or therms), Dollar amount billed, Other charges, Electricity Commodity Adjustment/Fuel Cost Adjustment, Taxes, Invoice total, and Invoice date

23 Xcel Energy Privacy Policy https://www.xcelenergy.com/staticfiles/xe/Admin/Xcel%20Online%20Privacy%20Policy.pdf

be supporting the program. Some of these groups have already begun planning for privacy-protective approaches to handling CEUD. For example, OPower specializes in energy data software and has incorporated *PbD* into its company's privacy principles,[24] including specific commitments by OPower to design and build security and privacy protections at every stage in their architecture and IT systems.[25] Tendril, which offers a platform so that energy software developers can build consumer energy applications,[26] intends to manage CEUD according to privacy best practices and lead their developer community into following the same.

Green Button

"Green Button" is the common-sense idea that electricity customers should be able to download their own energy usage data in an easy-to-use format.[27] It comes in response to a White House call-to-action, with the implementation being led by industry representatives. The aim of the initiative is for consumers to be better educated about their energy decisions and encourage consumers to make investments to reduce their energy costs. There are two facets to Green Button:

- *"Download My Data"* – CEUD goes directly from the utility to the customer. Most utilities in the U.S. are currently implementing this version of Green Button.
- *"Connect My Data"* – CEUD is transferred from the utility to a third party with the customer's consent and authorization.

Green Button incorporates privacy and security best practices, whereby electricity consumers can get access to their information only after authenticating themselves on a utility portal with a login and password.[28] In the case of the Download My Data function, that information is shared only with the consumer; if electricity consumers wish, in the future to share their CEUD with third parties they trust, they can do so with the Connect My Data function.

An Ontario Green Button initiative is currently being led by the MaRS Discovery District and the government of Ontario.[29] Several Ontario startups are emerging to service not only Ontario energy consumers, but energy consumers internationally. Ontario-based startups include Quinzee, Ecotagious, Project Neutral, Green Energy Watchdog, MMB Research, and Prolucid.[30] The Ontario Power Authority is also leading a request for proposal regarding social benchmarking pilot programs.[31]

---

24 Opower Implements Privacy by Design, Opower Press Release http://opower.com/company/news-press/press_releases/55

25 Opower's Data Principles http://opower.com/company/data-principles

26 Tentril http://www.tendrilinc.com/about/

27 Green Button http://www.greenbuttondata.org/

28 Energy Services Provider Interface http://www.naesb.org/ESPI_Standards.asp (Green Button is based upon the North American Energy Standards Board (NAESB) Energy Services Provider Interface (ESPI) software developer's kit.)

29 http://www.metering.com/node/21846

30 http://quinzee.ca/, www.ecotagious.com, http://projectneutral.org, www.greenenergywatchdog.com, http://mmbresearch.com, www.prolucid.ca

31 http://www.powerauthority.on.ca/rfp-social-benchmarking-pilot-program

SDG&E's Implementation of Green Button

In September 2011, the White House challenged the U.S. utilities to develop a tool to provide energy consumers easy access to their energy usage data. The "Green Button" is the resulting national initiative, introduced by the White House and developed by the energy industry. The idea is to ensure customers have timely access to their own energy data with the "click of a button."

San Diego Gas & Electric (SDG&E) has been an early and strong supporter of the Green Button's goal to provide consumers with ease of access and control over their CEUD, and to inspire innovative consumer applications and devices from entrepreneurs, businesses and students.

Green Button Download My Data

SDG&E was among the first utilities in the U.S. to launch Green Button "Download My Data," providing customers with easy access to their energy usage data. SDG&E saw the Download My Data option as giving customers the ultimate choice since it is completely up to the user on where to send their data. Also, customers can have the convenience of sharing their CEUD with a third party without the utility being in the middle of the transaction.

SDG&E launched Green Button Download My Data in December 2011. When looking at options for implementation, SDG&E's philosophy was to leverage their existing customer online portal as much as possible in order to utilize existing authorization and authentication tools. To allow this, SDG&E added the Download My Data function within the portal in the Energy Charts section of My Account. As such, when a customer logs in to the portal, they meet the necessary authentication procedure. Customers must sign up for My Account, using their account number from their energy bill, their zip code, and are then prompted to choose a username and password. By clicking on the Green Button Download My Data icon, customers can download 13 months of past energy consumption data in a standardized file format (Energy Services Provider Interface XML) for easy export to other applications, to developers, or to third parties.

One important lesson learned is the importance of both computer-friendly and consumer-friendly formats of Green Button data. Over the past year, SDG&E has received feedback that Green Button data should be both human-readable and machine-readable. This is rather easily accomplished with a style sheet, so that most browsers (including mobile/tablet ones) can present the data as human-readable. Experience has shown that there are a number of possible scenarios when people are going to want to take a look at the raw data as part of the process of sharing it. In short, it is important to place emphasis on 'usability' from the customer's perspective to develop customer-friendly options. Along those same lines, SDG&E has been working on simplifying the entire user experience around sharing this data, which has led to early support for Green Button Connect My Data.

Green Button Connect My Data

Green Button "Connect My Data" is an automated, more advanced level of the initial Green Button data download tool, and the next step in the industry-led Green Button initiative. To date, more than 10,000 customers have downloaded their energy consumption data with the SDG&E Green Button Download My Data tool. Through Green Button Connect My Data, customers can now authorize third parties to securely access their energy usage data, on an automated and daily basis. It is important to note that CEUD is only provided to third parties following affirmative action by the customer to send their CEUD to a particular destination. SDG&E takes the additional step of obfuscating the customer's ID before sending it to the third party.

Similar to the Download My Data function, Connect My Data is also available in the Energy Charts section of the SDG&E My Account customer web portal. Customers can view at any time within the My Account portal a list of third parties they have chosen to share their CEUD with, and are given the option to un-enroll from any automatic transfers to third parties at any time. Once a year, SDG&E will remind customers with which third parties they are currently enrolled.

On October 1, 2012, SDG&E and Candi Controls (subcontractor of Capgemini) announced the rollout of the Green Button Connect My Data platform with the launch of their first app, PowerTools. The new PowerTools app was demonstrated in Washington, D.C. at the 2012 Energy Datapalooza event.

PowerTools will help SDG&E customers to securely identify ways to make smarter choices in their energy use habits and decisions, improve efficiency and lower costs. Initially available for web browsers and mobile tablets, the app will soon also be available for additional platforms, including mobile phones and third party platforms such as Facebook. Highlights of the app's features include: historical usage analysis, overview of actual use and savings relative to history, environmental impact, ability to choose and track energy saving goals, utility bill payment, as well as other useful functionalities.

PowerTools is only the first app available via the Green Button Connect My Data platform. SDG&E anticipates expanding the platform to a variety of third parties (and apps) in 2013. In addition, SDG&E is continuing to look at potential future enhancements to the platform, including standardized application programming interface (API) implementation, support for a "privacy seal program," as well as additional information such as cost information at the interval level.

Conclusion

More than 23 million households around the world will participate in demand response programs by the year 2018.[32] Such trends towards the adoption of energy efficiency programs lead directly to the increased collection, use and disclosure of CEUD, resulting in a more efficient and reliable energy system. However, the manner in which CEUD is used by utilities and third parties is the subject of much discussion regarding its privacy implications.

In this paper, the Information and Privacy Commissioner of Ontario, Canada and the Future of Privacy Forum have sought to highlight the opportunities for innovation and the risks to privacy for greater access to CEUD by third parties. Companies offering innovative products and services can only do so if customers are able to have greater control over their CEUD. This includes allowing customers to download their CEUD in machine-readable format and disclose it to a third party of their choice, or to direct their utility to disclose their CEUD to a third party. Initiatives seeking to facilitate this include the Green Button and Future of Privacy Forum seal initiatives described in this paper.

Conversely, privacy considerations must be addressed in the areas of information technology, accountable business practices, and networked infrastructure when planning for third party access to CEUD. By adopting a *Privacy by Design* approach, third parties can ensure that privacy is proactively embedded within third party CEUD data flows, right from the outset.

32 http://www.businesswire.com/news/home/20121030005343/en/23-Million-Households-Worldwide-Participate-Demand-Response

Appendix – IPC PbD Smart Grid papers

Date	Title	Authors
November 2009	SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation	Ann Cavoukian, Ph.D. Information & Privacy Commissioner, Ontario, Canada Jules Polonetsky Co-Chair, Future of Privacy Forum Christopher Wolf Co-Chair, Future of Privacy Forum
June 2010	*Privacy by Design*: Achieving the Gold Standard in Data Protection for the Smart Grid	Office of the Information & Privacy Commissioner of Ontario Hydro One Toronto Hydro Corporation
February 2011	Operationalizing *Privacy by Design*: The Ontario Smart Grid Case Study	Office of the Information & Privacy Commissioner of Ontario Hydro One GE IBM TELVENT
March 2012	Applying *Privacy by Design* Best Practices to SDG&E's Smart Pricing Program	Ann Cavoukian, Ph.D. Information & Privacy Commissioner, Ontario, Canada Caroline Winn Chief Customer Privacy Officer, San Diego Gas & Electric
April 2012	Smart meters in Europe: *Privacy by Design* at its Best	Ann Cavoukian, Ph.D. Information & Privacy Commissioner, Ontario, Canada Foreword by Alexander Dix, LL.M. Commissioner for Data Protection and Freedom of Information Berlin, Germany
May 2012	Building Privacy into Ontario's Smart meter Data Management System: A Control Framework	Independent Electricity System Operator (IESO) Office of the Information and Privacy Commissioner Ontario, Canada

Office of the Information and Privacy Commissioner, Ontario, Canada

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

Web site: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

January 2013

SDGE connected
A Sempra Energy utility

Information and Privacy Commissioner, Ontario, Canada

THE FUTURE OF PRIVACY FORUM