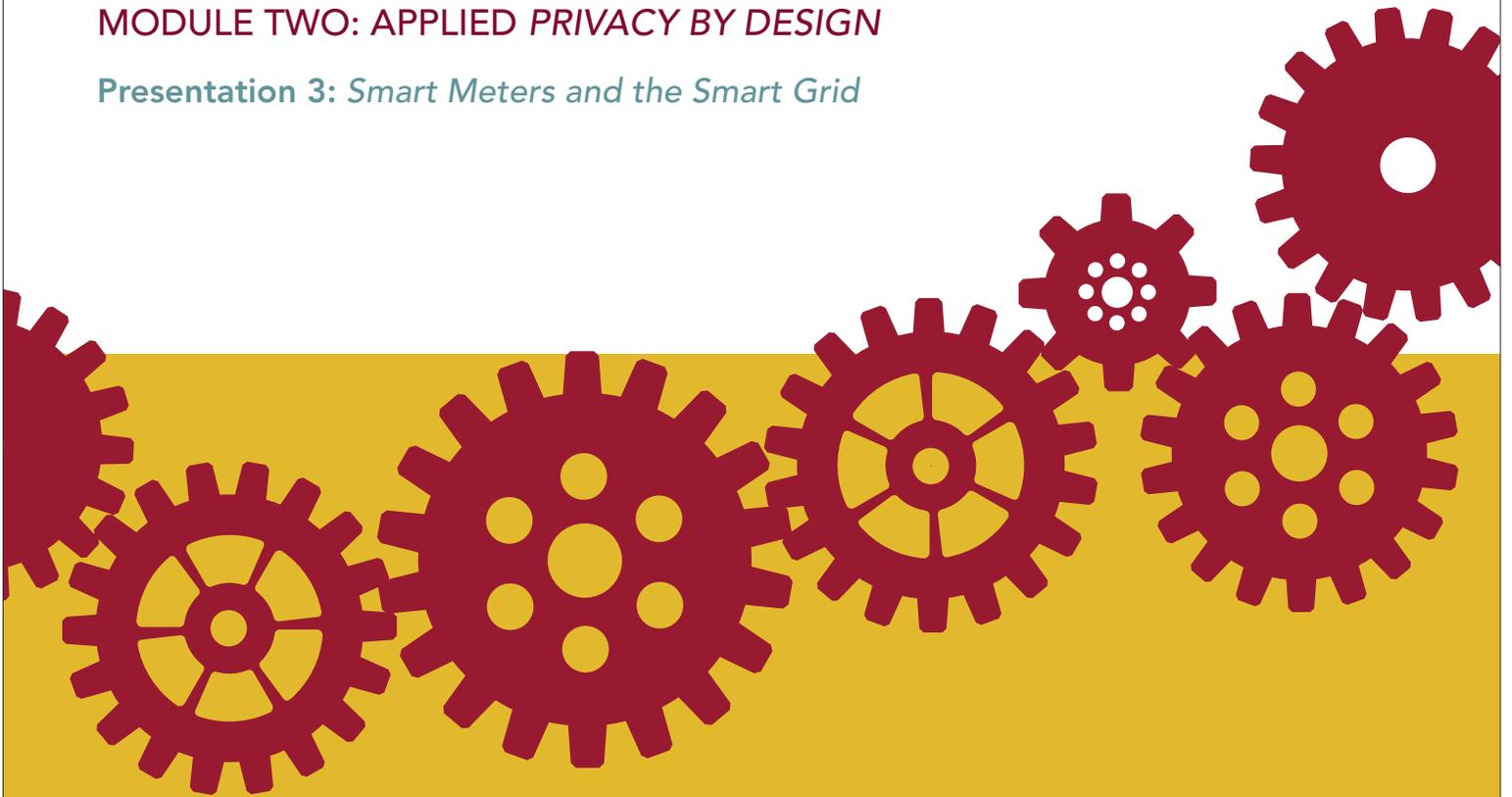


Privacy by Design Curriculum 2.0

Instructor Resources

MODULE TWO: APPLIED PRIVACY BY DESIGN

Presentation 3: Smart Meters and the Smart Grid



CONTENTS

Overview	2
Essential Reading	2
Learning Objectives	2
<i>The Smart Grid: Overview of Presentation</i>	3
Further Reading	4
Presentation Materials with Instructor Notes	5



Overview

This section describes the Smart Grid and identifies some key areas of privacy risk associated with it. It proposes best practices for designing privacy directly into the Smart Grid based on The 7 Foundational Principles of *Privacy by Design* and outlines two examples of how two major electrical utilities are implementing these practices.

Essential Reading

Information and Privacy Commissioner, Ontario and The Future of Privacy Forum, [SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation](http://www.ipc.on.ca). www.ipc.on.ca

Information and Privacy Commissioner, Ontario, Hydro One, & Toronto Hydro, [Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid](http://www.ipc.on.ca). www.ipc.on.ca

Information and Privacy Commissioner, Ontario, Hydro One, GE, IBM & Telvent, [Operationalizing Privacy by Design: The Ontario Smart Grid Case Study](http://www.ipc.on.ca). www.ipc.on.ca

Marek Jawurek, Martin Johns, Florian Kerschbaum, [Plug-in privacy for Smart Metering billing](http://www.arxiv.org). www.arxiv.org

Learning Objectives

Participants will understand the fundamentals of the Smart Grid and the privacy risks associated with it, and see how Ontario utilities are applying the principles of *Privacy by Design* to manage those risks.

Smart Meters and the Smart Grid

Overview of Presentation

Slide	Title	Theme
3.1	The Challenge	Building consumer trust
3.2	The Smart Grid: What is It?	A two-way flow of information and electricity in real time
3.3	Sample Smart Grid: Ontario	The Smart Grid, from generation to distribution to transmission
3.4	Imagining the Future: Elements of the Smart Grid	Smart meters, load management, smart appliances, dynamic pricing, and access to information about electricity consumption
3.5	One's Home – the Most Private of Places	Smart Grid technologies will make it possible to collect more granular data than ever before
3.6	Key Privacy Risk Areas	Key risks: 1) wireless transmission of data 2) collection, use, and disclosure of personal information 3) online access to consumer data.
3.7	Setting the Standard	Building on a solid foundation
3.8	Smart Grid Privacy by Design	Ontario, Canada's leadership in <i>Privacy by Design</i> for the Smart Grid
3.9	Best Practices	The 7 Foundational Principles of <i>Privacy by Design</i> in the Smart Grid context
3.1	Simple Application of <i>PbD</i> : Online Customer Information Request	A simple example of how <i>Privacy by Design</i> can be built directly into Smart Grid systems.
3.11	Advanced Application of <i>PbD</i> : Load Management Program	An advanced example of how <i>Privacy by Design</i> can be built into Smart Grid systems
3.12	The Big Picture: A Privacy Perspective on the Smart Grid	Understanding privacy in the grid, customer, and services domains
3.13	Benefits of Proactively Embedding Privacy at the Design Stage	Building consumer confidence and trust, supporting conservation goals, and achieving cost savings

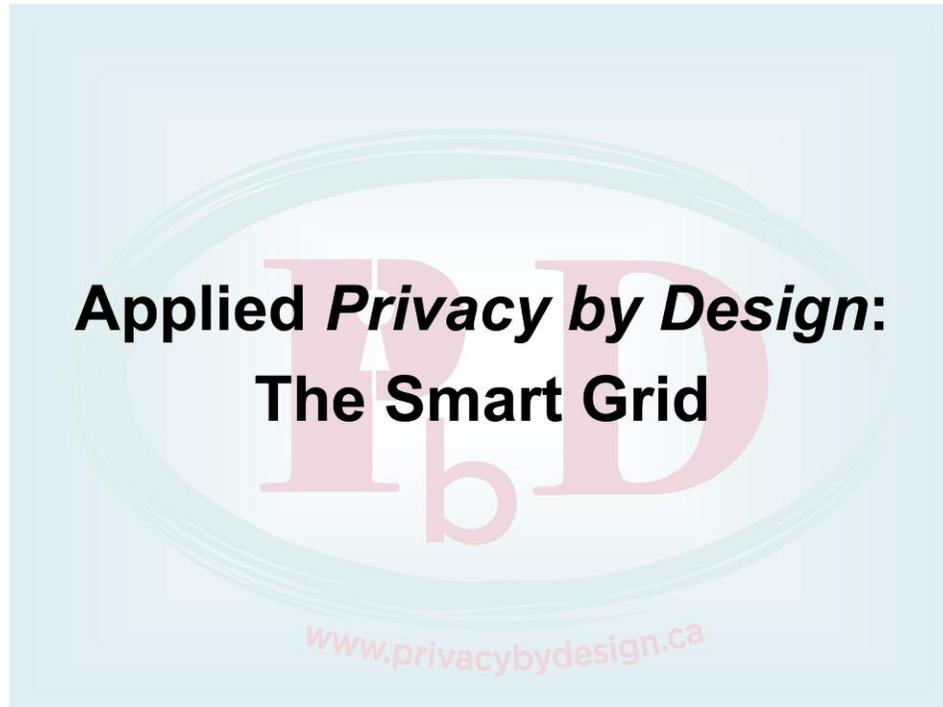
Further Reading

U.S. Department of Energy, [The Smart Grid: An Introduction](http://www.energy.gov). www.energy.gov

Modern Energy Review, www.modernenergyreview.com

Ecoalign, [A Day in the Life of a Customer in 2015: Visualizing The Smart Grid](http://www.ecoalign.com).
www.ecoalign.com

Presentation Materials with Instructor Notes



Slide 1

The Challenge

“In order for the Smart Grid to grow and become truly successful, it will *have* to engender consumer confidence, trust, and respect for user privacy.”

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

www.privacybydesign.ca

Slide 2

As countries around the world move to modernize their electrical grids in the face of growing demands, many are making efforts to make the grid “smarter.”

The Smart Grid presents new opportunities for growth and change. And while there may be widespread enthusiasm for electricity reform, it is important that we recognize that the Smart Grid will make it possible to collect more granular data than ever before about customers’ energy consumption. Information proliferation, lax controls, and insufficient oversight could lead to unprecedented invasions of consumer privacy.

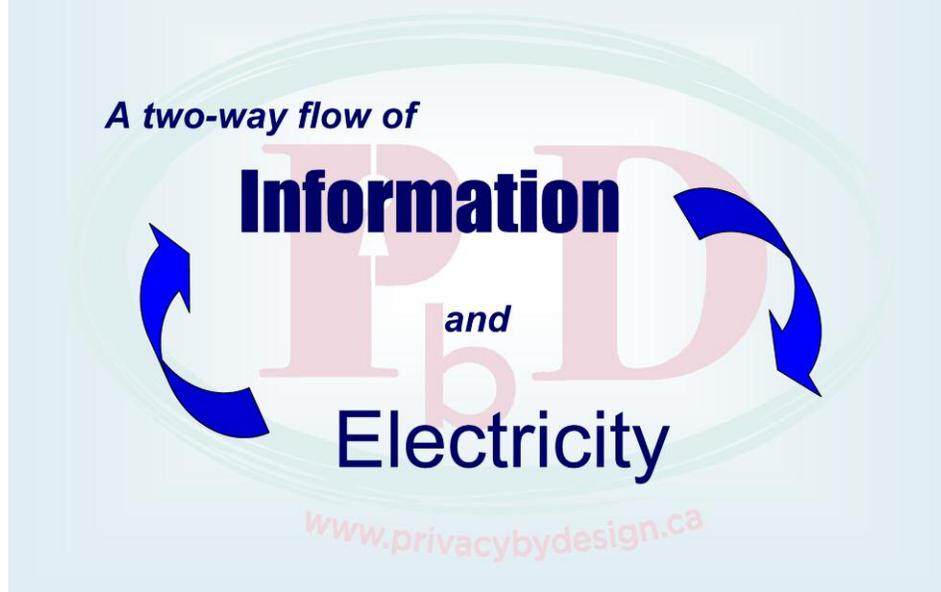
An Accenture survey conducted in 22 countries revealed that 32% of consumers do not trust energy companies, and 46% trust them only when they have direction from government (Accenture New Energy World Survey, 9 March 2010: <http://newsroom.accenture.com>). Utilities clearly have an interest in ensuring that consumer adoption of Smart Grid energy saving programs is not impeded by fears relating to privacy.

Significantly, customers' relationships with power utilities are generally borne out of necessity. Unless a person can generate their own power, they must either obtain power from a utility or go without it. Practically speaking, there is no opt out from energy suppliers.

As a result, is it especially incumbent on utilities to build privacy into the design and implementation of Smart Grid technologies and processes.

Managing data responsibly, in a trustworthy and transparent manner, will help build confidence in the Smart Grid, and allow both utilities *and* consumers to reap the benefits of its implementation.

The Smart Grid: What is it?



Slide 3

In general terms, the Smart Grid refers to the modernization of the electrical grid, such that there is a two-way flow of information and electricity.

Communications technology and infrastructure are at the heart of the Smart Grid, which will combine data provided by smart meters, sensors, computer systems and other devices, and allow consumers and utilities to act on the basis of that data.

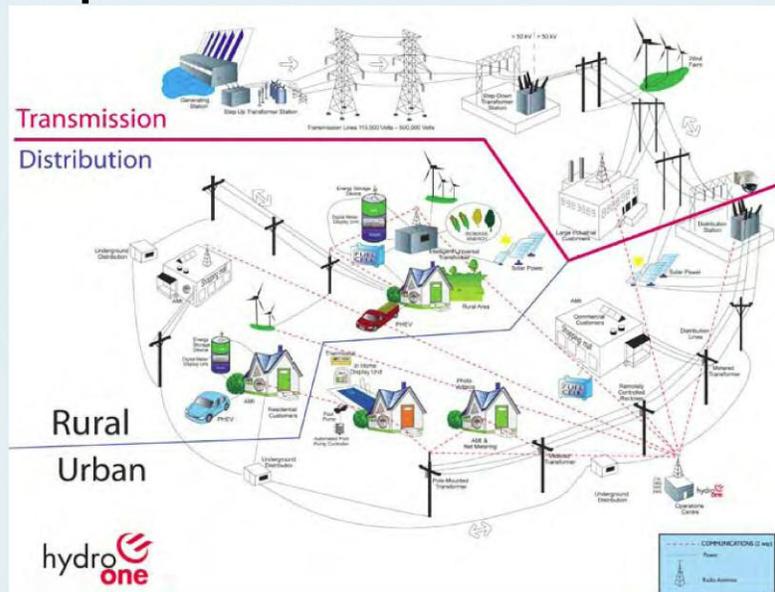
Benefits of the Smart Grid may include:

- Improved reliability of power and reduction of outages;
- Greater ability to deploy environmentally-friendlier power sources;
- Self-repair, which may, among other things, improve public and electricity worker safety;
- Enablement of new load management, distributed generation, energy storage, and demand-response options;

- Reduced vulnerability to terrorist attacks and natural disasters;
- Reduction of future capital expenditure requirements because “bits are cheaper than iron.”

As part of delivering on these benefits, the Smart Grid infrastructure may ultimately allow consumers – and utilities – to track energy consumption day-to-day, even at the appliance level.

Sample Smart Grid: Ontario



Slide 4

Understanding the privacy risks associated with the Smart Grid, and working to minimize those risks, requires an appreciation of how the Smart Grid will function. Of course, the particular details will vary from one jurisdiction to another. But this diagram shows a simplified model of Ontario's Smart Grid that is useful in understanding the foundational concepts relevant to most Smart Grids.

When we talk about the Smart Grid, we are talking about the application of new technologies and processes throughout the electrical grid: at the level of the generation and bulk transmission of electricity, and also at the level of distribution and consumption.

In this diagram, we see electricity generation and bulk transmission in the top area labelled "Transmission." In many countries, the Smart Grid involves expanding into new and/or renewable sources of electricity. Currently, we cannot conceive of privacy issues associated with **bulk** energy generation and transmission because there is no personal information involved (and therefore no role for privacy).

Lower down in this diagram we can see where electricity is used in homes and businesses. Importantly, it may also ultimately be generated there, for example, through solar panels that can produce energy to be sold back to the utility.

This is where devices such as smart appliances and smart meters bring personal information into play. Here, Smart Grid technologies may enable the collection of personal information at an unprecedented level of granularity. So it is very important that the collection, use, disclosure and disposal of this information be managed appropriately from the outset in order to protect customer privacy.

Imagining the Future: Elements of the Smart Grid



Slide 5

Different jurisdictions will implement the Smart Grid in different ways. In most jurisdictions, it is still too soon to tell exactly what the Smart Grid will look like when it is fully deployed. Nevertheless, some common elements are likely to be found in jurisdictions around the world:

Smart meters: can record and report electricity consumption information automatically. Smart meters identify consumption in greater detail than a conventional meter and communicate that information back to the electrical utility for monitoring and billing purposes. They can relay detailed information to the utility on a daily, hourly or real-time basis.

Load management: will grant control of a customer's smart appliances such as air conditioners, water heaters, and pool pumps to the utility company so it can reduce or smooth demand for electricity during peak energy demand periods. In a load management scenario, the smart meter also becomes an entry point for information – in the form of instructions – from the utility into the home.

Smart appliances: can include thermostats, washers, dryers, microwaves, hot water heaters, and refrigerators that can communicate with the utility. A smart thermostat, for example, can receive instructions from the utility to adjust the temperature to reduce energy consumption during peak hours.

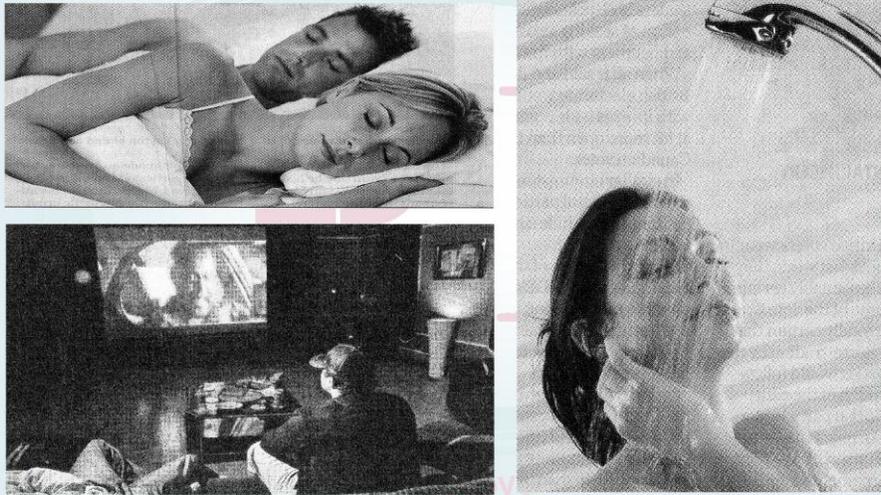
Dynamic pricing: is an economic incentive that uses technology to provide pricing information for current or future time periods, and allows the customer to modify demand in accordance with price.

Dynamic pricing can take the form of:

- *Time-of-use pricing:* Energy prices are higher at pre-designated peak times and lower at others.
- *Critical peak pricing:* Where the rate is set much higher for the most critical peak hours.
- *Real-time pricing:* Where prices vary by the hour according to the utility's cost to purchase or produce the energy.

Consumer access to energy-related information. Consumers will have access to energy pricing and usage information using tracking tools and software applications. Electricity providers and others are also setting up their own customer web interfaces. These make data collected via the smart meter and smart appliances available to consumers to support decision-making about how much electricity they use, and when.

Home: The Most Private of Places



Images – Toronto Star/Shutterstock – May 12, 2010

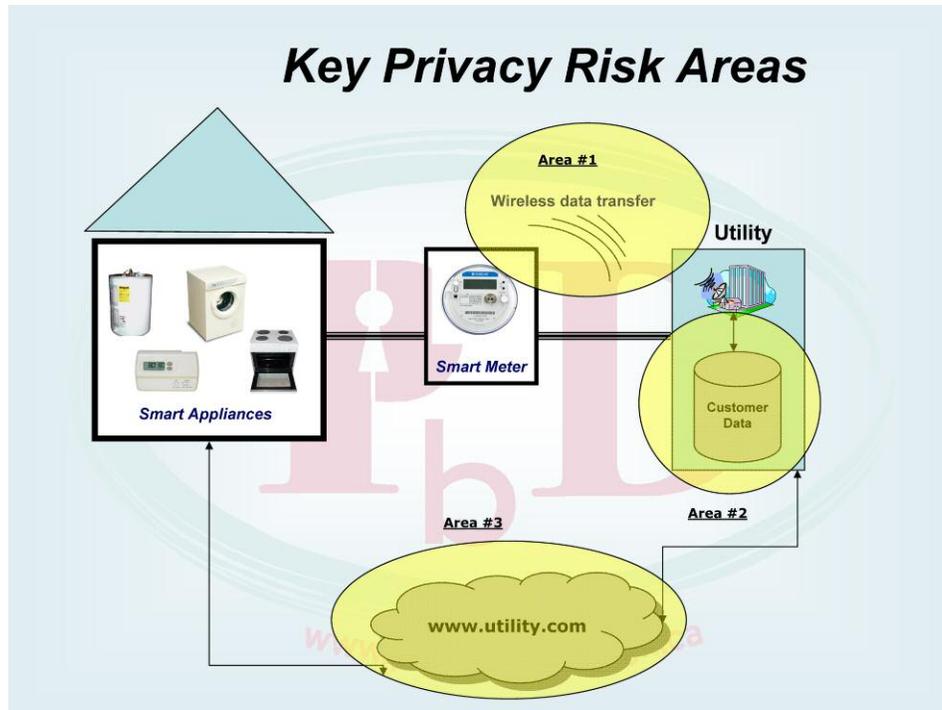
Slide 6

Clearly, while the Smart Grid may offer many potential benefits, it also raises concerns from a privacy point of view as a result of its potential to collect very detailed data about the use of electricity inside the homes of individual customers.

As smart appliances and devices become part of the grid, it will be possible, for example, to collect very granular data about:

- Whether you have breakfast;
- Whether you cook in the microwave or on the stove;
- What time you get home in the evening;
- Whether you have an alarm system and whether it is activated;
- Whether appliances are in good condition;
- Whether and how often exercise machines are used;
- Whether and how often you watch television; and
- What time you usually shower.

This kind of information can be combined with other data, such as work location and hours, and family status, to derive all kinds of assumptions that may be of interest to insurers, marketers, social service workers, and criminals.



Slide 7

Looking at this simplified model of the Smart Grid, we can identify 3 key areas of privacy risk. Developing a good understanding of specific Smart Grid plans in your own jurisdiction will help you identify other possible areas of concern. For example, depending on how they are deployed, smart appliances may raise important privacy issues (e.g. if they communicate directly with the utility).

Risk Area 1 is the point at which home consumption data, collected via smart appliances, is transmitted to the utility, and where the utility may also transmit data, some of which may be personal data, to the smart meter. The transfer may be wired or wireless. The risks here relate to the granularity of the data and the fact that the data may be intercepted, for example, by hackers or others with malicious intent, and that as a result personal information may be compromised or erroneous/false instructions communicated to the smart meter and smart appliances.

Risk Area 2 pertains to the collection, use, disclosure, and disposal of customer information by the utility, including billing and detailed consumption information. As we've seen, this data may be very granular in nature, which opens up risks of its being used for secondary purposes by the utility or by third parties, including data matching, marketing, profiling, etc. It may also be vulnerable to theft or hacking.

Risk Area 3 relates to the online consumer access points to energy consumption data held by the utility. These websites, which will help consumers understand how and when they are using electricity, will need strong security and authentication measures to prevent unauthorized access to this potentially sensitive data.

Setting the Standard

“At the end of the day, it’s all about standards. If we get that right at the outset, we create an ecosystem for the development of technologies that will thrive in the present and future.”

Chuck Adams, President of IEEE
(Institute of Electrical and Electronics Engineers)

www.privacybydesign.ca

Slide 8

Clearly, it is important to get privacy “right” at this early stage in the development of the Smart Grid.

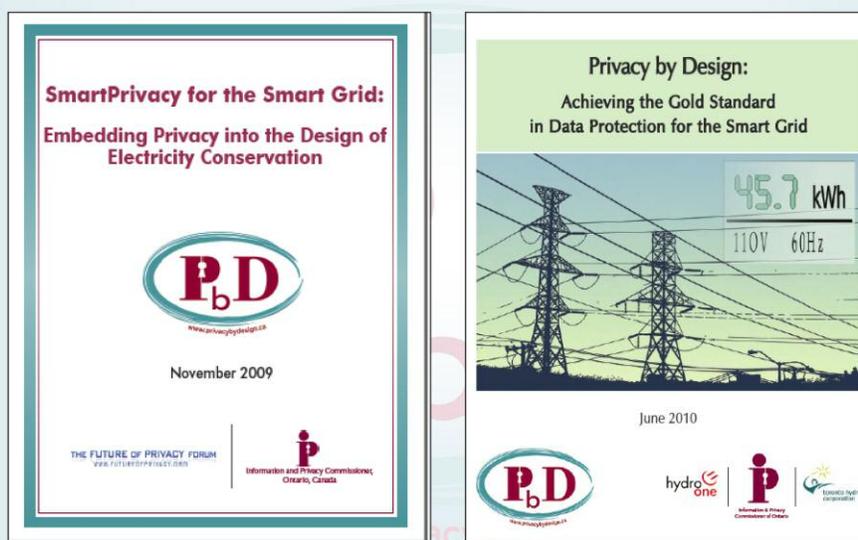
Accomplishing the goals of the Smart Grid while simultaneously achieving privacy protection requires adopting a positive-sum model, whereby functionality and privacy can coexist in a win-win scenario for both.

Building privacy measures into the Smart Grid need not weaken functionality but can, in fact, enhance the overall design of the system. This is particularly true now, as the system is in its infancy. This is the time to build privacy proactively into the system, right from the outset.

That’s the essence of *Privacy by Design*, and its effect is to minimize the unnecessary collection and uses of personal data by the system, strengthen data security, and empower individuals to exercise greater control over their own information.

Building privacy in at this early stage, from the ground up, will establish the right environment for engendering consumer trust and confidence in the Smart Grid, and allow its benefits to be realized.

Smart Grid *Privacy by Design*



Slide 9

As utilities all over the world work toward making their grids smarter, privacy issues must be at the forefront of their design work.

In 2009, the Ontario Information and Privacy Commissioner released a paper entitled *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*. This paper called attention to the privacy risks related to the Smart Grid, and argued that energy conservation could be achieved without sacrificing the privacy of energy customers. The paper posited a positive sum paradigm, where one value need not be sacrificed in support of another.

In June 2010, the Commissioner issued a Best Practices guide for applying *Privacy by Design* to the Smart Grid. The paper was a joint project with leading Ontario energy companies Hydro One Networks Inc. and Toronto Hydro Electric System. It was designed to serve as a roadmap for utilities worldwide.

In the Best Practices guide, *Privacy by Design* is put forward as the standard to be adopted in Smart Grid implementation, and examples are given of how Smart Grid programs in Ontario, Canada are being built with *Privacy by Design* as a central guiding design feature.

Best practices

The Smart Grid shall:

1. Be proactive, not reactive
2. Build in privacy as the default
3. Embed privacy into its design
4. Avoid false trade-offs between objectives
5. Build in privacy end to end
6. Be visible and transparent
7. Treat consumer privacy as a core functional requirement

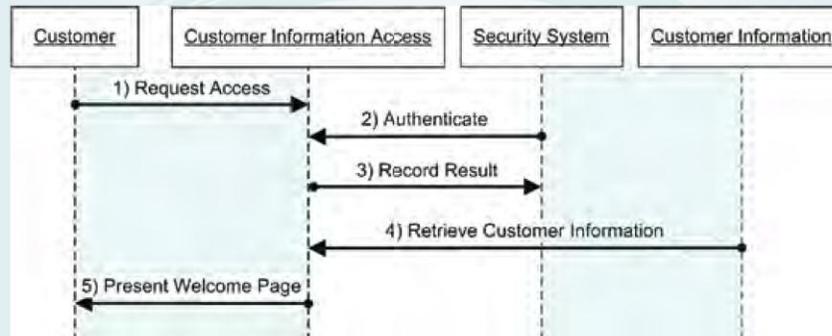
www.privacybydesign.ca

Slide 10

1. Smart Grid systems should feature privacy principles in their overall project governance framework and proactively embed privacy requirements into their designs right from the project inception phase. This means including the 7 Foundational Principles of *Privacy by Design* in the requirements development and design processes, and building and testing systems for alignment with those requirements.
2. Smart Grid systems must ensure that privacy is the default so that no action is required on the part of the consumer to protect his or her personal information.
3. Smart Grid systems must make privacy a core functionality in the design and architecture of systems and practices – it must be an essential design feature.
4. Smart Grid systems must accommodate all legitimate interests and objectives in a positive-sum, win-win manner and avoid unnecessary zero-sum trade-offs.

5. Smart Grid systems must build in privacy end-to-end, throughout the entire life cycle of any personal information collected;
6. Smart Grid systems must be able to demonstrate how privacy has been incorporated into their design in a way that is transparent to consumers by engaging in accountable business practices and ensuring that new systems operate according to stated objectives.
7. Smart Grid systems must be designed with respect for consumer privacy as a core foundational requirement to enhance consumer confidence and trust.

Simple Application of *PbD*: Online Customer Information Request



Sequence Diagram for Customer Information Access

From IPC, Toronto Hydro and Hydro One, *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid*, p. 21

Slide 11

This first example is a simple but important one, showing how Ontario utilities are building privacy into how customers access information about their energy consumption online.

The customer must first enrol in the program. On subsequent visits, they must then be authenticated prior to access. In the diagram above, we see how authentication functions in a privacy-enabled way.

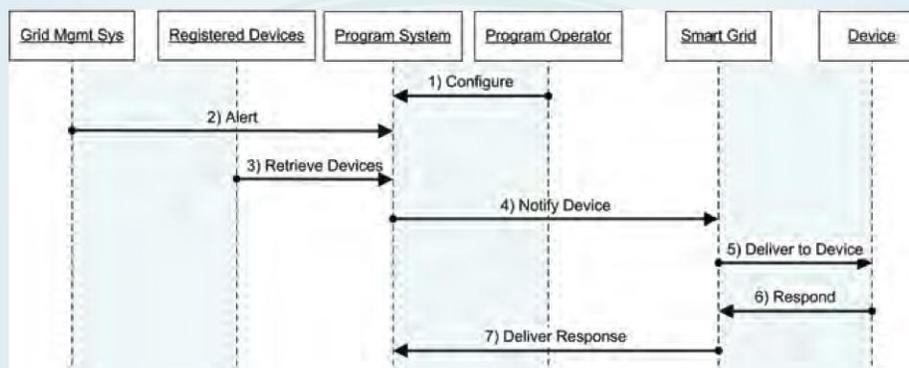
The steps are shown in the diagram above:

1. The customer provides his/her unique identifier and access information, such as a password.
2. The customer information access will require that the identifier and password information be verified. If correct and the account is in working order (e.g. it has not been disabled due to multiple access attempt failures), then the customer is considered to be authenticated.

3. The successful access is recorded/logged.
4. The basic information regarding the authenticated customer is retrieved.
5. The customer is presented with the user interface.

This example illustrates the requirement that all customers be authenticated. Steps 2, 3, and 4 show how privacy has been built into the system through the authentication requirements to help protect against unauthorized disclosure of personal information via the website.

Advanced Application of *PbD*: Load Management Program



**Sequence Diagram for Usage
(Part of Customer Enablement in the Smart Grid)**

From IPC, Toronto Hydro and Hydro One, *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid*, p. 24

Slide 12

The second use case scenario shows a utility in the process of rolling out smart meters and billing system changes to support time-of-use billing, which will include further customer enablement. Examples of future customer enablement include demand-response programs, conservation programs, voluntary curtailment, advanced device management, in-home displays, and many others.

For the purpose of this use case scenario, consider the case of customers choosing to participate in demand-response programs, such as when there is a peak in power-demand and some customers have opted to make their thermostats available for a 2 degree Celsius reduction. The success of a customer engagement program hinges on the utility's ability to empower willing customers to become active participants in their energy use and generation.

The process proceeds as shown in the diagram above:

1. **Alert received** — The Smart Grid continually monitors the stability of the network and events are generated whenever problems occur (i.e. if demand approaches supply).

2. **Retrieve Devices** — Based on configured rules in the demand response program, the system will determine how many devices – like thermostats or smart meters – have to be adjusted to meet the demand requirement need. At this point, the system is completely agnostic to specific customer data. It will retrieve device information from the registration system and will be limited to the device identifier and user constraints (e.g. minimum/maximum temperatures).

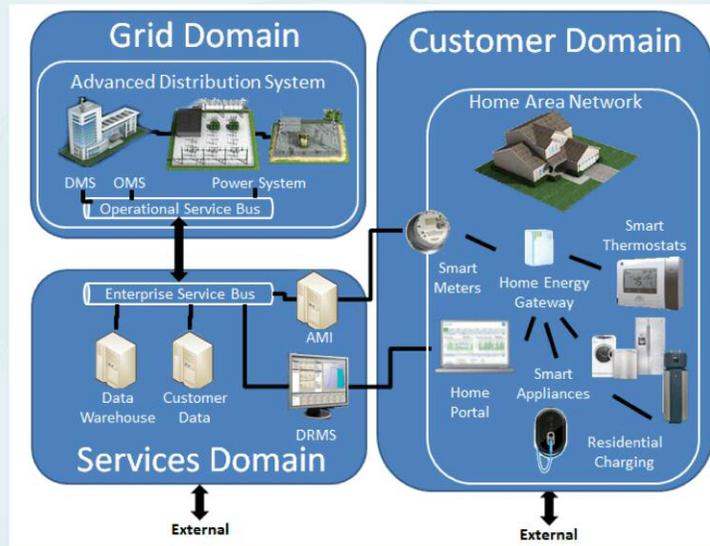
Note: This is the essential step for the supplemental requirement to “Limit Data.”

3. **Notify Device** — The demand response system will request all the devices where the tolerances are allowable to change their temperature settings.
4. **Deliver to Device** — The Smart Grid ensures that the device is authenticated and the message is delivered securely to the device.
5. **Respond** — Depending on the technology, a response will be provided to the request.
6. **Deliver Response** — The Smart Grid ensures that the response is delivered to the demand response program system. The information is limited to an acknowledgement and state of action requested.

The fundamental concept that underlies the entire flow is that the operating system executing demand response operations is completely blind to any of the specific, identifiable details of a given individual. Personally identifiable information is a function of program enrolment, but this association operates separately from device management. In other words, the system running the Smart Grid only knows the rules for the management of devices based on the program it is associated with, and is completely agnostic to the particular details of a given customer.

This distinction demonstrates several tenets of the Smart Grid *Privacy by Design*. The segregation of data is proactively embedded directly into the system design and privacy is the default.

The Big Picture: A Privacy Perspective on the Smart Grid



Slide 13

The third paper in the Ontario Information and Privacy Commissioner's Smart Grid series is *Operationalizing Privacy by Design: The Ontario Smart Grid Case Study*, which showcases the approach taken by Hydro One and its vendor partners, IBM, GE and Telvent, in their "Living Lab" Smart Grid deployment

A key outcome of operationalizing *Privacy by Design* in this deployment is the clarification of three domains of the Smart Grid:

- 1.) The Grid Domain, which relates to systems and processes to manage the power network;
- 2.) The Customer Domain, which incorporates all the devices in the consumer's home; and
- 3.) The Services Domain, which includes customer service functions such as billing and demand management programs.

This analysis provides the conceptual framework for understanding how personal information can be limited to the domains where it is relevant, thereby containing potential privacy risks. This is an important underpinning to embedding privacy appropriately, and also to minimizing risk by limiting personal information to the domains where it is truly necessary.

In the paper, specific examples are provided of design requirements for minimizing and protecting personal information in each domain while achieving full system functionality in a positive sum, not zero sum, manner.

Benefits of Embedding Privacy at the Design Stage

- ✓ Clarification of relationship between business and privacy requirements
- ✓ Good business practice that enhances consumer confidence and trust
- ✓ Supports energy conservation by removing barriers to consumer participation
- ✓ Cost-effective and secure

www.privacybydesign.ca

Slide 14

The growth and success of the Smart Grid requires consumer confidence and trust in the technology and its implementation. Utilities play an essential role in building that trust by demonstrating respect for user privacy.

Embedding privacy at the design stage is quite simply good business. Personal information can be a significant liability to organizations that don't manage it effectively. Privacy breaches can cost millions, and the trust that is lost through the mishandling of personal information is challenging to regain.

By contrast, being proactive about privacy helps support consumer trust, and in this case, will help utilities implement Smart Grid initiatives successfully so that the goals of the Smart Grid, which include conservation and security, can be realized, and privacy respected. This is far more effective and efficient than awaiting public outcry and then trying to add privacy on later.

By thinking through the privacy risks now, early in the process, we can ensure that privacy is built in from the ground up, in a cost-effective and holistic way. Doing so will help support consumer confidence in the Smart Grid, and allow the energy and efficiency benefits of the Smart Grid to be reaped without sacrificing privacy.

More information and a growing library of resources are available at

www.privacybydesign.ca

www.privacybydesign.ca

Slide 15