Smart Energy: Operationalizing Privacy

Ken Anderson
Assistant Commissioner (Privacy)
Ontario

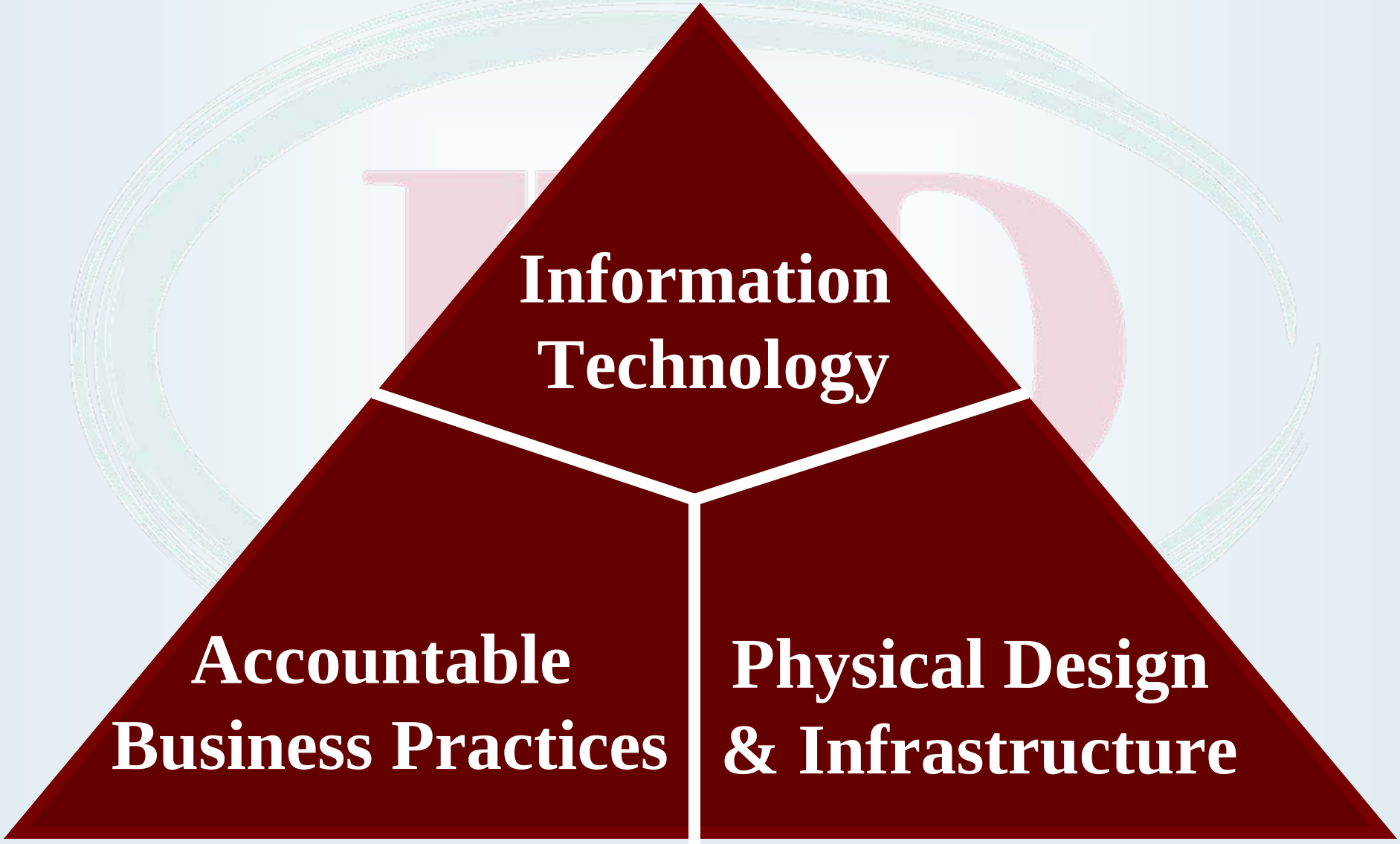
Smart Energy Canada
February 15, 2011

Presentation Outline

1. *Privacy by Design: The Gold Standard*
2. *Smart Grid: Bigger than the Internet?*
3. *Smart Privacy for the Smart Grid*
4. *Addressing Challenges*
5. *Best Practices for the Smart Grid*
6. *Use Case Scenario for the Smart Grid*
7. *Operationalizing Privacy by Design across the Smart Grid*

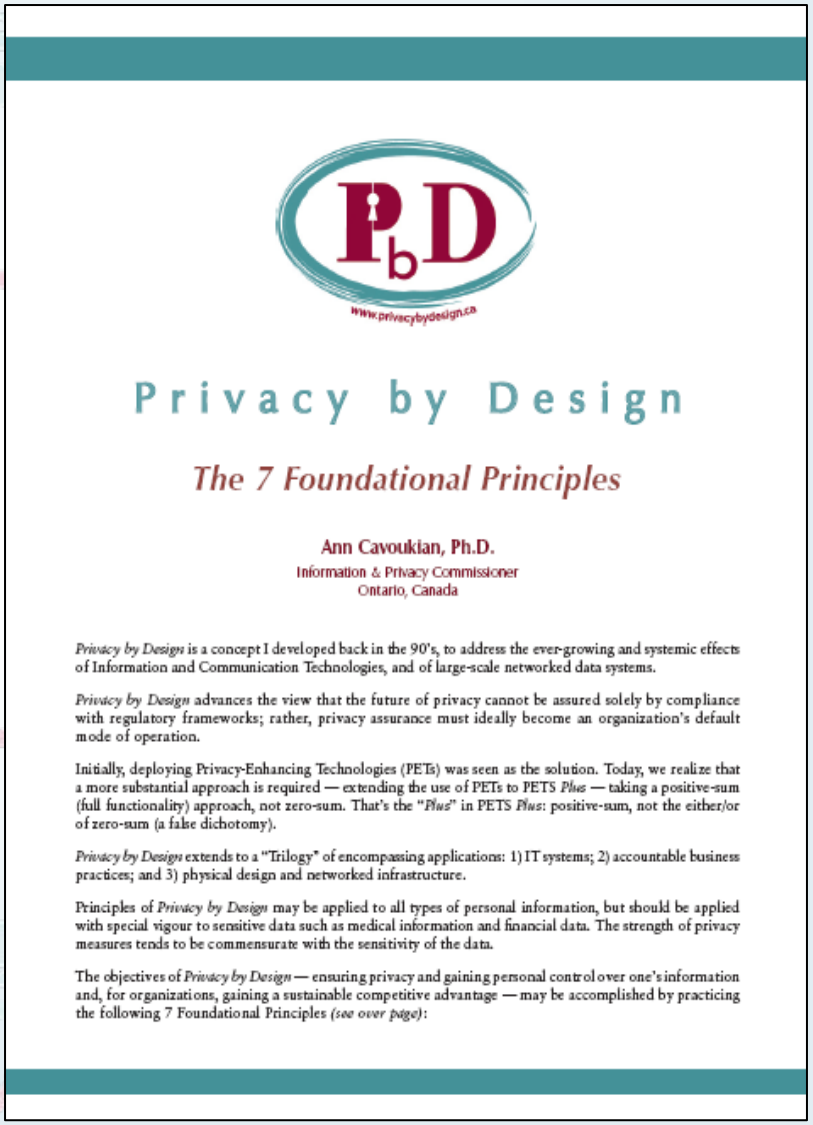

PbD
www.privacybydesign.ca

Privacy by Design:
The Trilogy of Applications



Privacy by Design:
The 7 Foundational Principles

1. ***Proactive*** not ***Reactive***;
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.



PbD

www.privacybydesign.ca

Privacy by Design

The 7 Foundational Principles

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

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

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

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

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

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

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

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

Smart Grid:
"Bigger than the Internet"

"Our expectation is that this network will be 100 or 1,000 times larger than the Internet. If you think about it, some homes have Internet access, but some don't. Everyone has electricity access – all of those homes could potentially be connected."

— Marie Hattar,

V.P. Cisco Network Systems Solutions,

Cisco: Smart grid will eclipse size of Internet, CNET news.

http://news.cnet.com/8301-11128_3-10241102-54.html

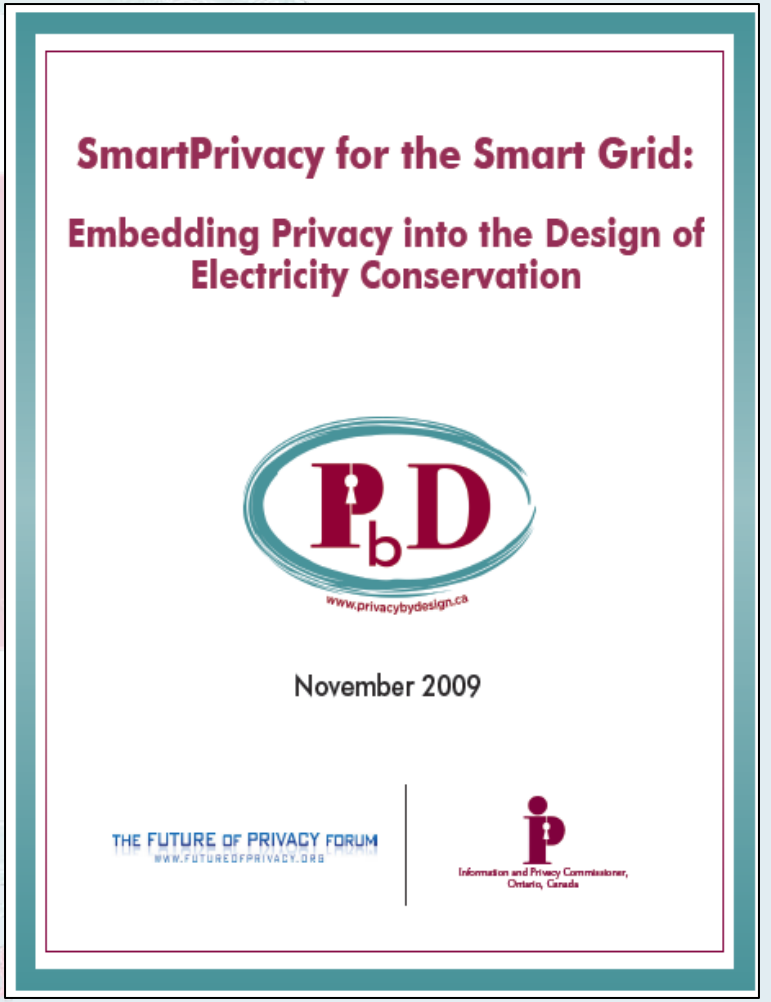
Why Utilities Should Care About Privacy

- ***Consumer confidence and trust is lacking:***
- Residents of Marin, California, created a road blockade that prevented PG&E trucks from going into their town to install smart meters;
- These residents were worried about privacy, with one saying, *"I don't want to be watched all the time;"*
- **79%** of people know little or nothing about the smart grid; **76%** don't know anything about smart meters (*Market Strategies International Study*, 2010);
- As a result, consumers are wary, and at times, hostile.

SmartPrivacy for the Smart Grid:
Embedding Privacy into the Design of Energy Conservation

"The smart grid is certainly a good idea, which I strongly support. But the focus has been so singularly on controlling energy use that I think the privacy issue is a sleeper – it is not top-of-mind."

— Commissioner Cavoukian, Toronto Star, *Smart grid saves power, but can it thwart hackers?*, August 3, 2009



www.privacybydesign.ca

"Assets Beyond the Meter — Who Should Own Them?"

"There are sound reasons why energy consumers should remain in control of the energy consumption information they produce, even if there isn't a law that requires this. The underlying rationale is that consumer confidence and trust in the Smart Grid, and in one's local electricity distributors, is ***vital*** *in achieving the vision of a more energy efficient electrical grid."*

— Commissioner Cavoukian,
Electric Light & Power Magazine
www.elp.com

Changes Utilities are Experiencing

- **While a significant portion of the Smart Grid will not involve consumer information, the amount of personal information being collected and the digital nature of that information will precipitate internal changes within utilities that go well beyond individual IT departments;**
- Impacts of the Smart Grid as they relate to consumers include the primary operation areas of home energy management, metering, and demand-side management;
- The amount of data available from smart metering and Smart Grid devices will grow substantially and may require a significantly more robust means of validating, storing and filtering this data for optimal use;
- New technologies may be introduced arising from changes experienced by utilities in implementing the Smart Grid: Smart energy regulators, capacitors, switches and power line monitors to support energy conservation by reducing energy losses, distributed generation penetration, plug-in vehicles, and improved reliability and management of utility assets.

Personal Information on the Smart Grid

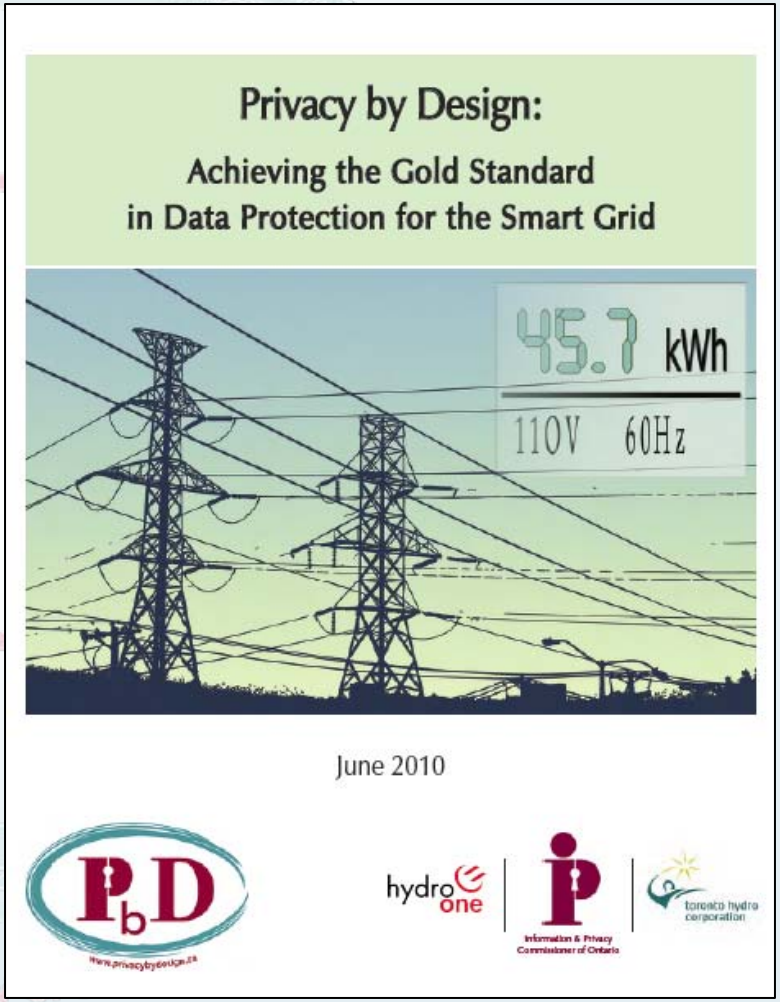
- What constitutes “personal information” on the Smart Grid is the subject of much discussion;
- Personal information is defined by the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), as ***“recorded information about an identifiable individual;”***
- Once it becomes apparent that a Smart Grid technology, system or project will involve the collection of personal information, either directly or through some form of data linkage, privacy considerations immediately apply;
- Digitization - Digital smart meter data, like all digital data, is vulnerable to accessing, copying, matching, merging and widespread dissemination.

Addressing Challenges

- Utilities will find opportunities to adopt ***Privacy by Design*** when introducing new technologies into the development of the Smart Grid, integrating communications, operational and information systems, as well as updating business processes.

Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid

- The Smart Grid in Ontario
- Personal Information on the Smart Grid
- *Privacy by Design*: The Gold Standard
- ***Best Practices for the Smart Grid: Think Privacy by Design***
- Smart Grid *Privacy by Design* Use Case Scenarios



www.privacybydesign.ca

Best practices for the Smart Grid
Privacy by Design

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 – prevent the harm from arising;
2. Smart Grid systems must ensure that privacy is embedded as the default – the "no action required" automatic mode of protecting consumers' privacy – its presence must be ensured;

Best practices for the Smart Grid
Privacy by Design (Cont'd)

3. Privacy must be made a core functionality in the design and architecture of Smart Grid systems and practices – an essential design feature;

4. Smart Grid systems must avoid unnecessary, zero-sum trade-offs between privacy and legitimate objectives of Smart Grid projects – adopt a positive-sum paradigm;

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

Best practices for the Smart Grid
Privacy by Design (Cont'd)

6. Smart Grid systems must be visible and transparent to consumers – engaging in accountable business practices – ensuring that new systems operate according to open, 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.

Use Case Scenario for

Smart Grid *Privacy by Design:*

Customer Enablement

Customer Enablement covers the end-to-end scope of a customer's interaction with a utility's technology systems and processes involving three basic activities:

1. **Enrollment:** The ability for eligible customers to enroll and define their participation in programs offered by the utility;
2. **Usage (Operation):** The active operation and management of participating customers. This refers to the daily functioning of systems and processes for a utility to deliver the service;
3. **Termination:** The ability for customers to freely terminate their active participation – freedom of choice.

Use Case Scenario:

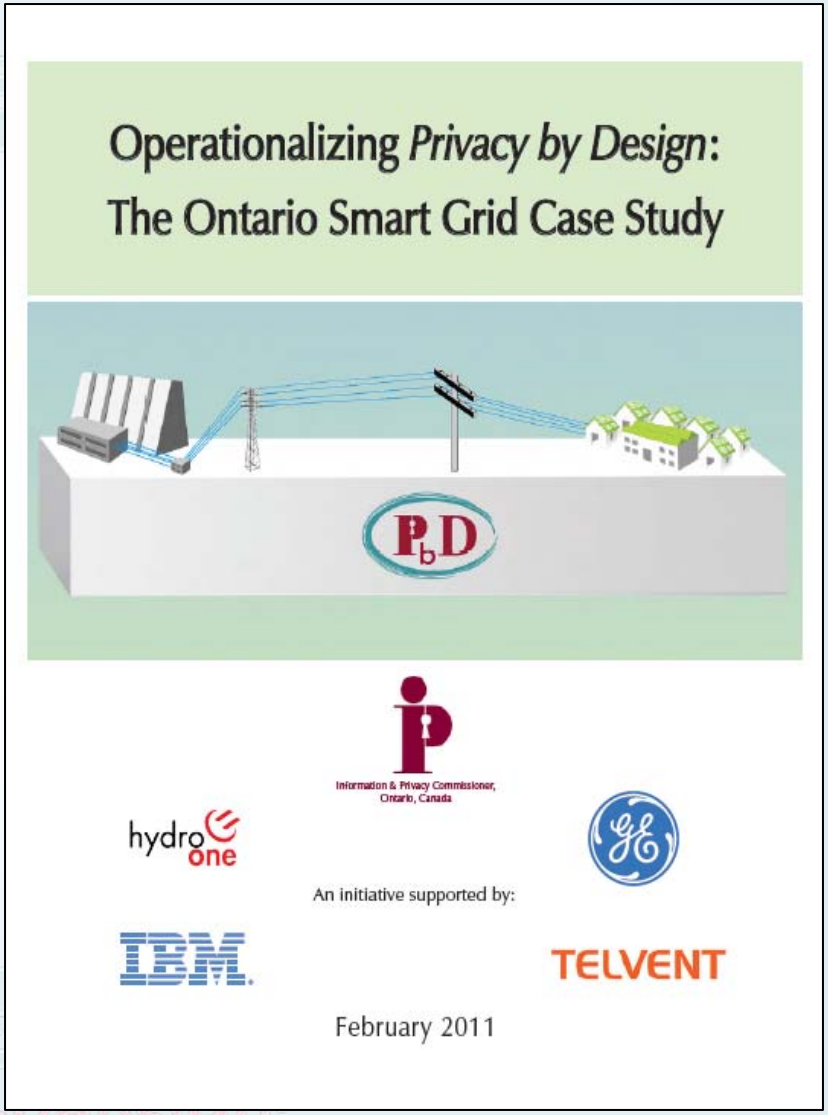
Details Relating to Usage

- A demand response system must determine how many consumer thermostats need to be adjusted;
- The system retrieves thermostat device information from the registration system, limiting the information retrieved to device identifier and user preferences (e.g. maximum/minimum temperature);
- The system collects ***no*** consumer data (e.g. name, telephone number, addresses, etc);
- Personally identifiable information is only needed for program enrolment, which operates separately from device management.

New IPC Smart Grid Paper

Operationalizing *Privacy by Design* into Hydro One's Smart Grid:

- Methodology for Operationalization;
- Operationalizing *Privacy by Design* across Smart Grid Domains;
- Working with partners – Hydro One, GE, IBM, Telvent.

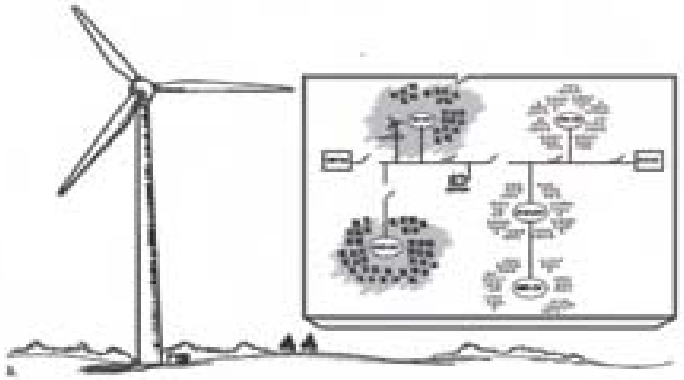


www.privacybydesign.ca

Advanced Distribution Solution (ADS)

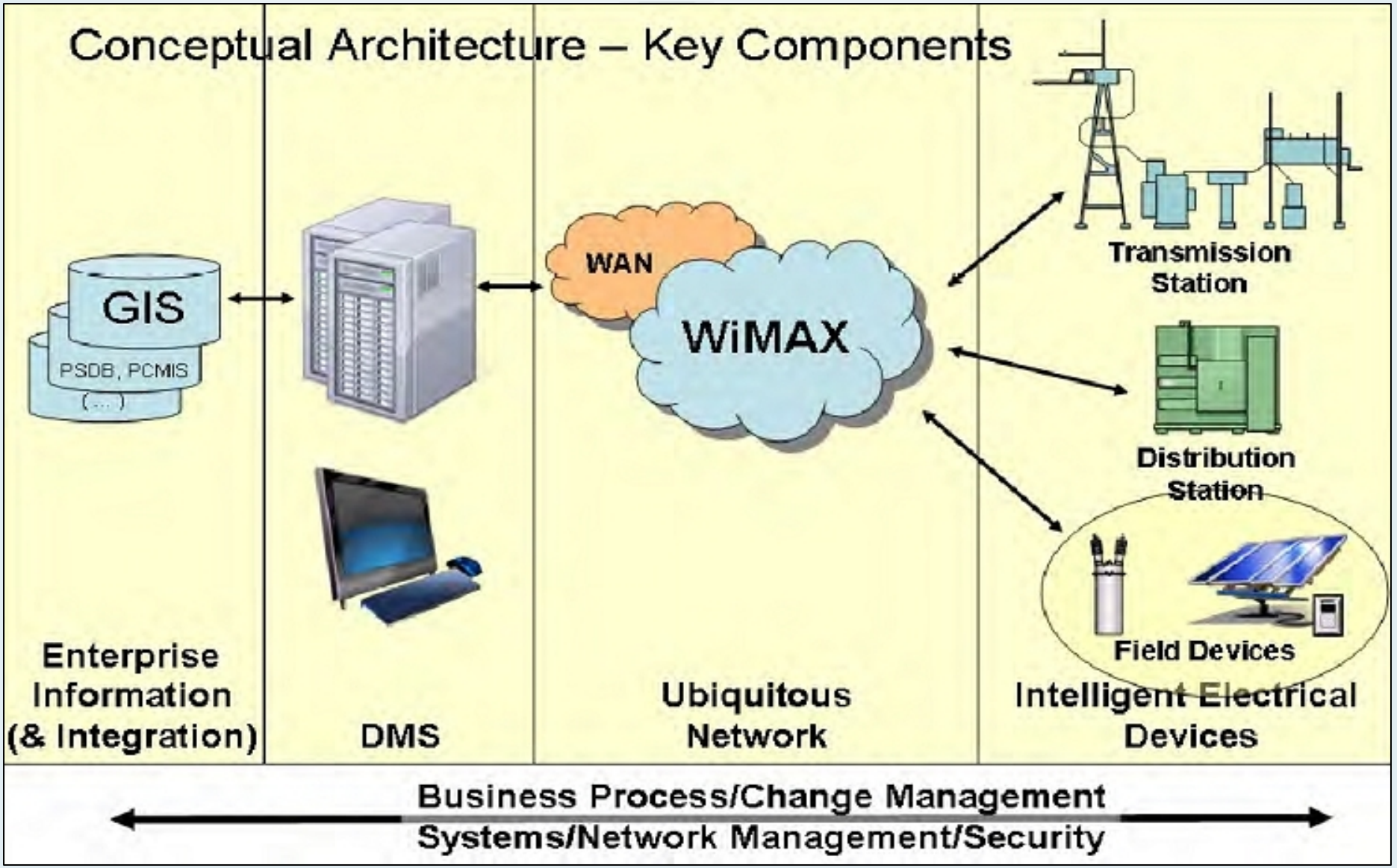
ADS has 4 Business Objectives

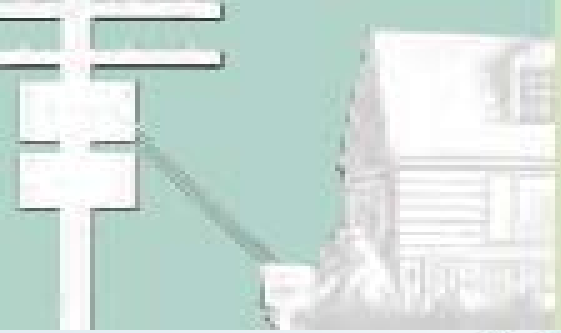
1. Optimize Connection of Distributed Generation (DG) on the Distribution Network
2. Improve Distribution Reliability and Operations
3. Optimize Outage Restoration
4. Optimize Network Asset Planning



hydro one

Architecture



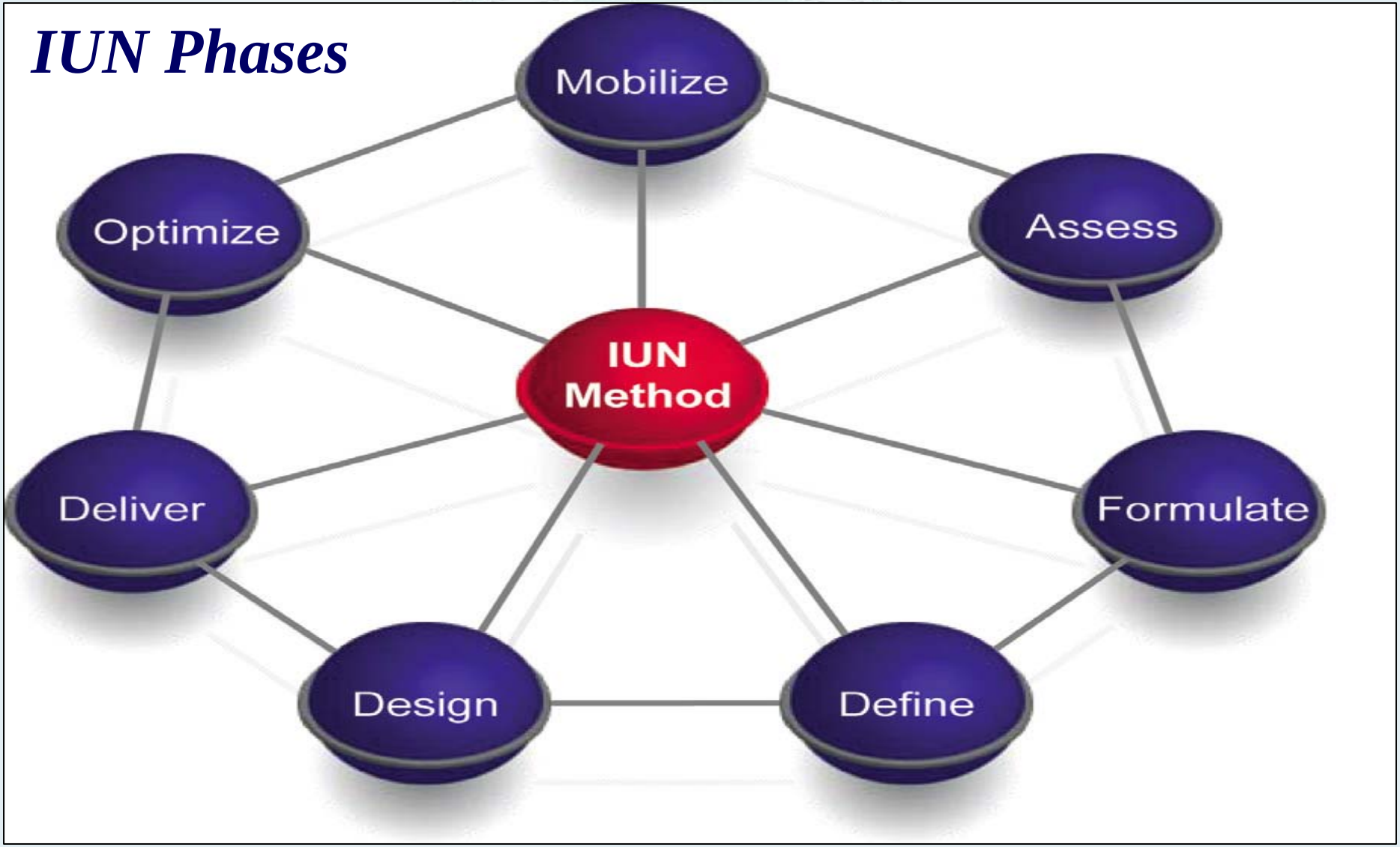


Operationalizing *Privacy by Design* into Hydro One's Smart Grid

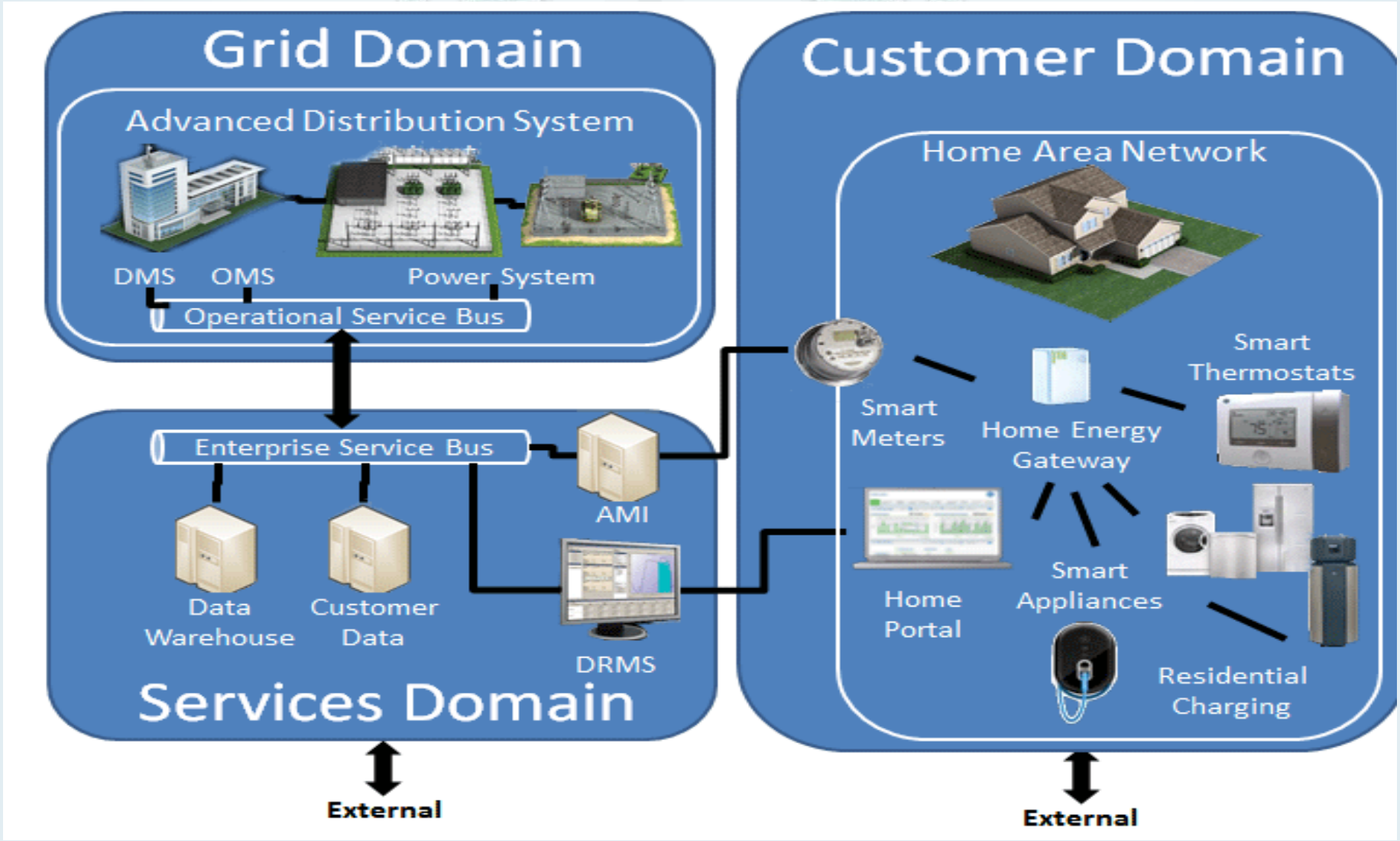
Smart Grid systems should:

1. Feature privacy principles in their project governance framework;
2. Ensure that privacy is the default;
3. Make privacy a core functionality;
4. Avoid any trade-offs between privacy and legitimate objectives;
5. Build in privacy end-to-end, throughout the entire data life cycle;
6. Be visible and transparent to consumers;
7. Be designed with respect for consumer privacy.

Methodology for Operationalizing *Privacy by Design* into Hydro One's Smart Grid



Operationalizing *Privacy by Design* across Smart Grid Domains



Discussion

Q's & A's

How to Contact Us

Ken Anderson
Assistant Commissioner (Privacy)

IPC Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada

M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca