Take the Lead: Embed *Privacy by Design* into the Emerging Smart Grid

Ken Anderson

Assistant Commissioner of Privacy

Ontario

January 31, 2011

Electric Light & Power EXECUTIVE CONFERENCE

www.elpconference.com

"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.

Imagining the Future: Elements of the Smart Grid

Smart Meters

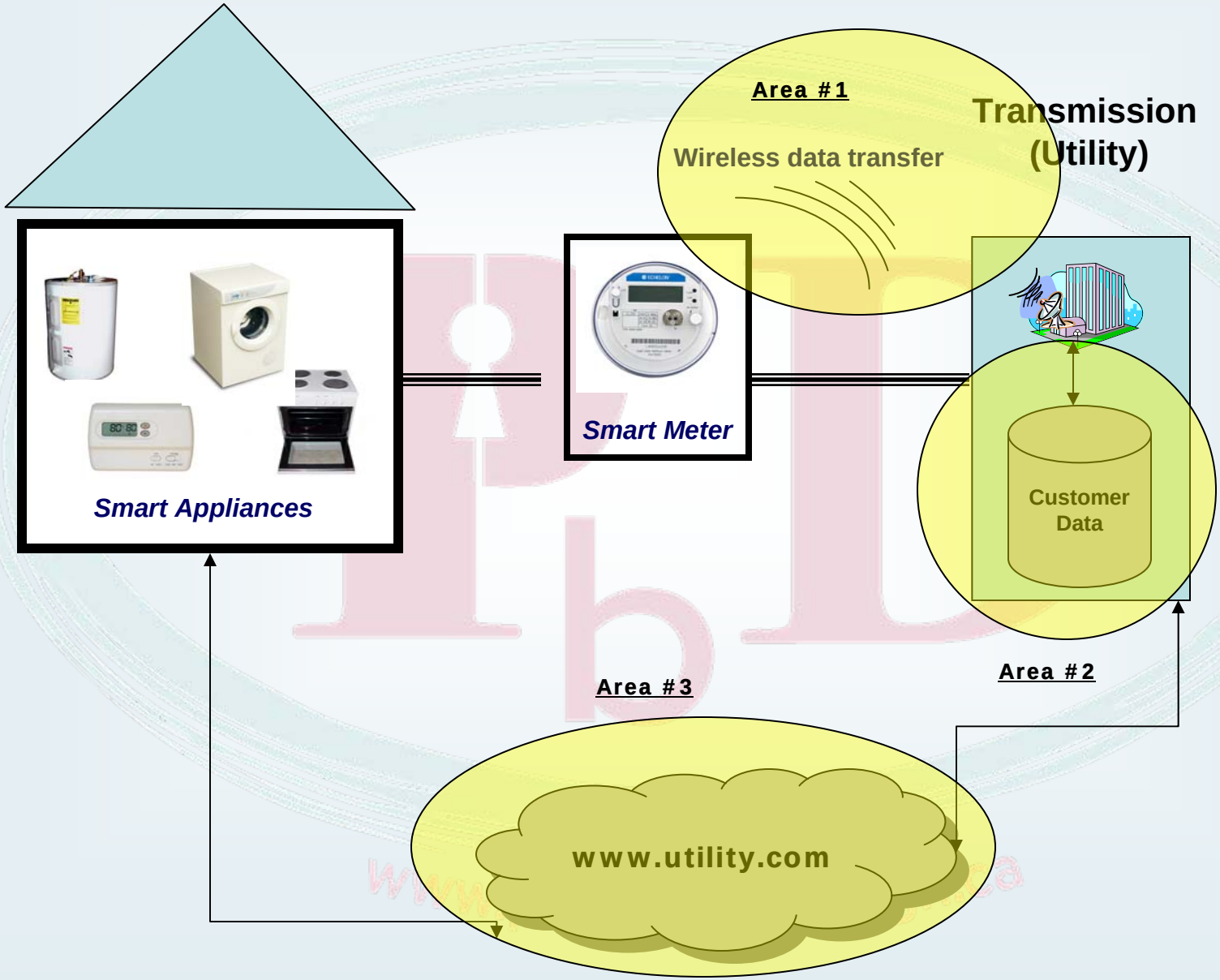
Load Management

Smart Appliances

Dynamic Pricing

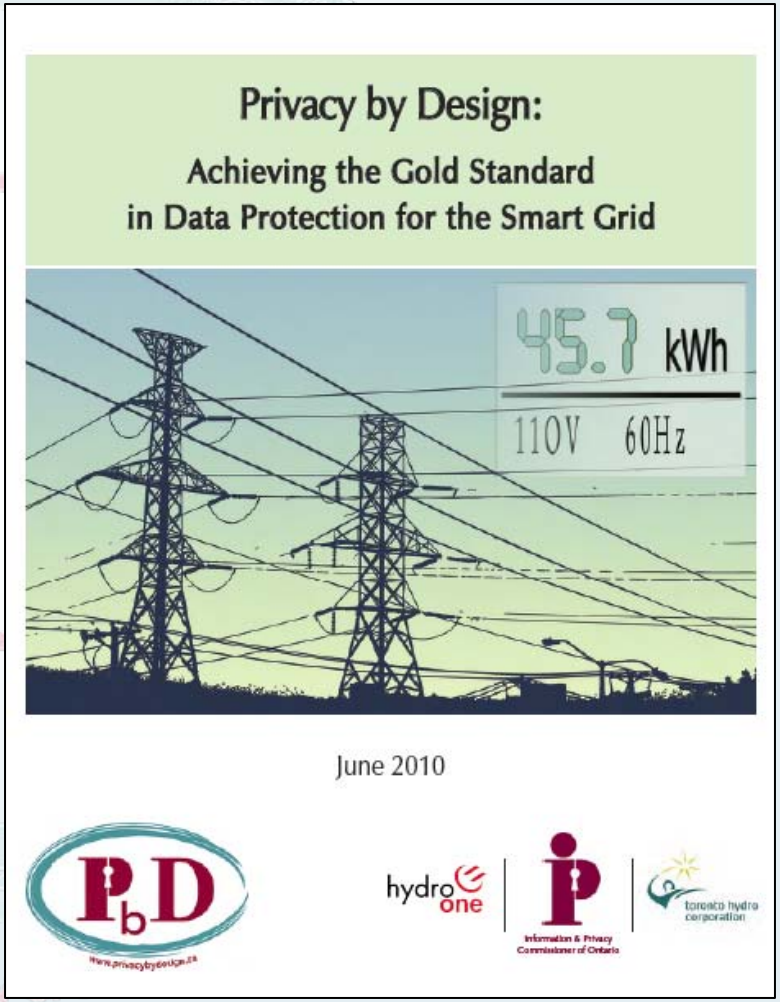
Access to Energy Information

Key Privacy Risk Areas



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:

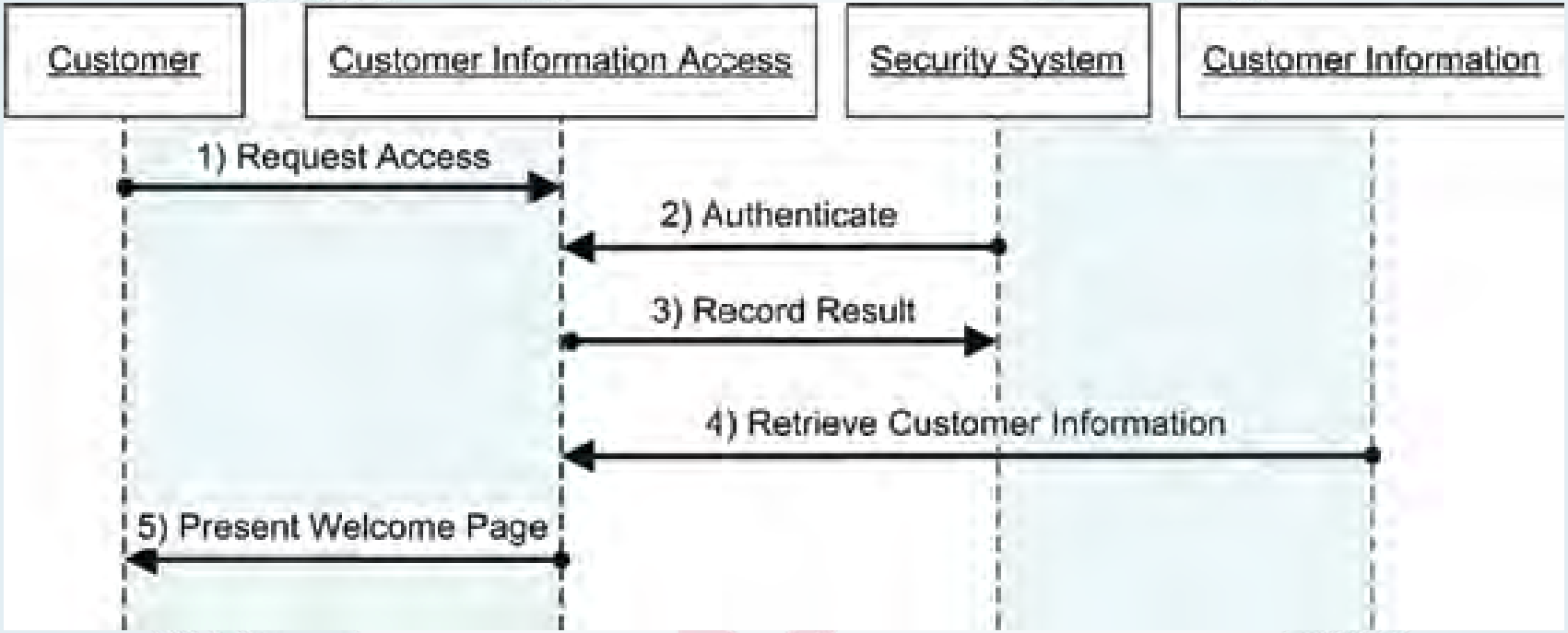
1. **Enrollment:** The ability for eligible customers to enroll and define their participation in programs offered by the utility;
2. **Usage (Operation):** The active operation and management of participating customers. This refers to the daily functioning of systems and processes for a utility to deliver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

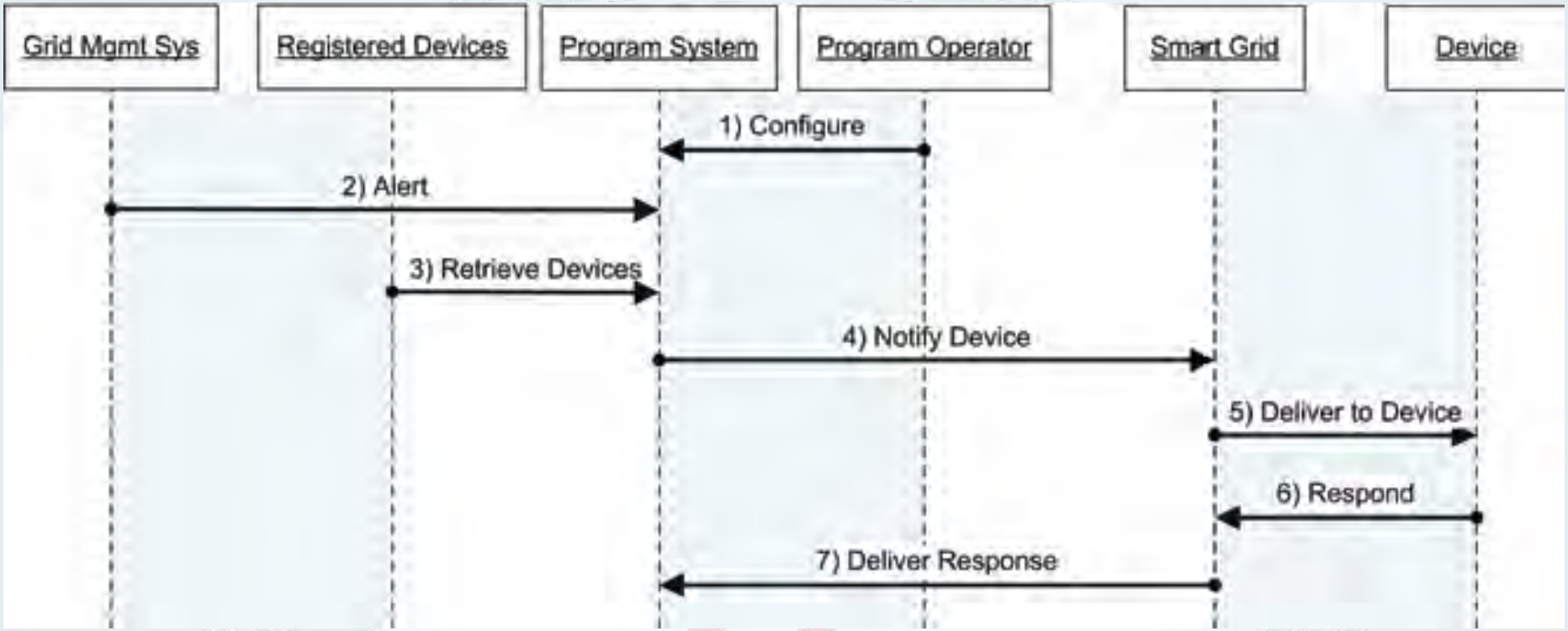
Simple Application of *PbD*: Online Customer Information Request



Sequence Diagram for Customer Information Access

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

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 fro the Smart Grid*, p. 24

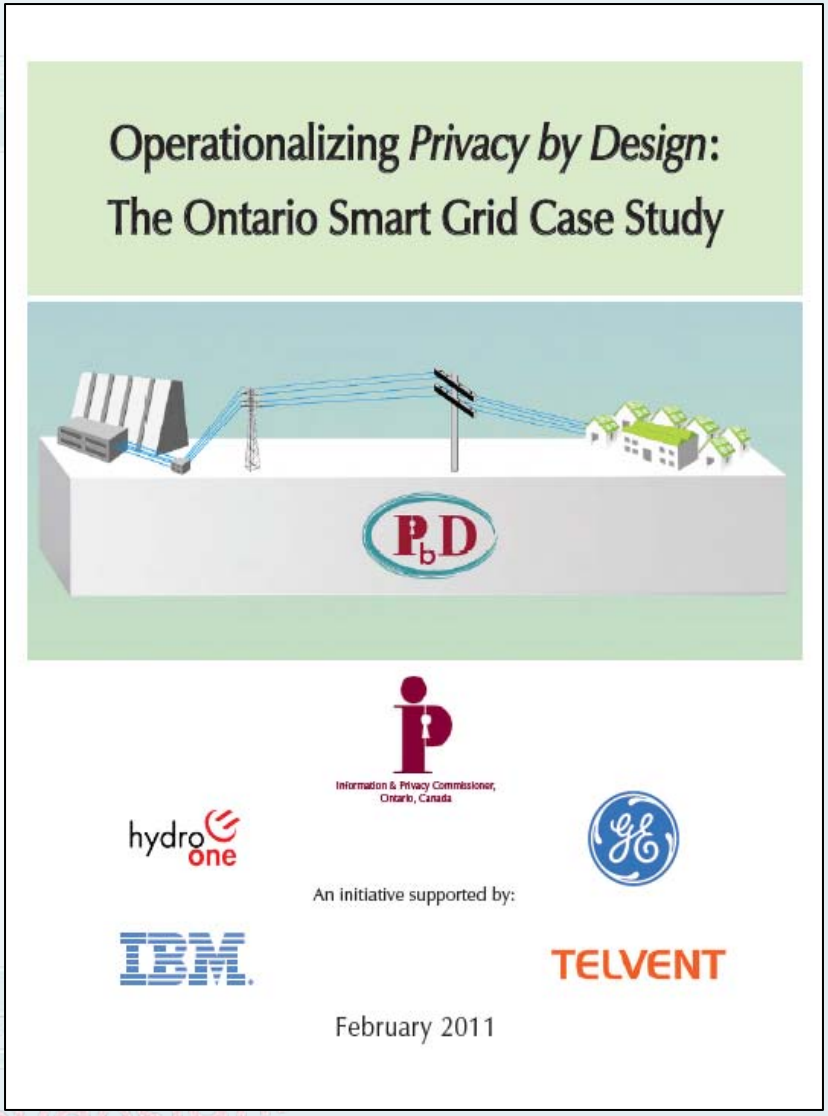
Benefits of Embedding Privacy at the Design Stage

1. **Good business practice that enhances consumer confidence;**
2. **Supports conservation by removing barriers to consumer participation;**
3. **Cost-effective.**

New IPC Smart Grid Paper

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

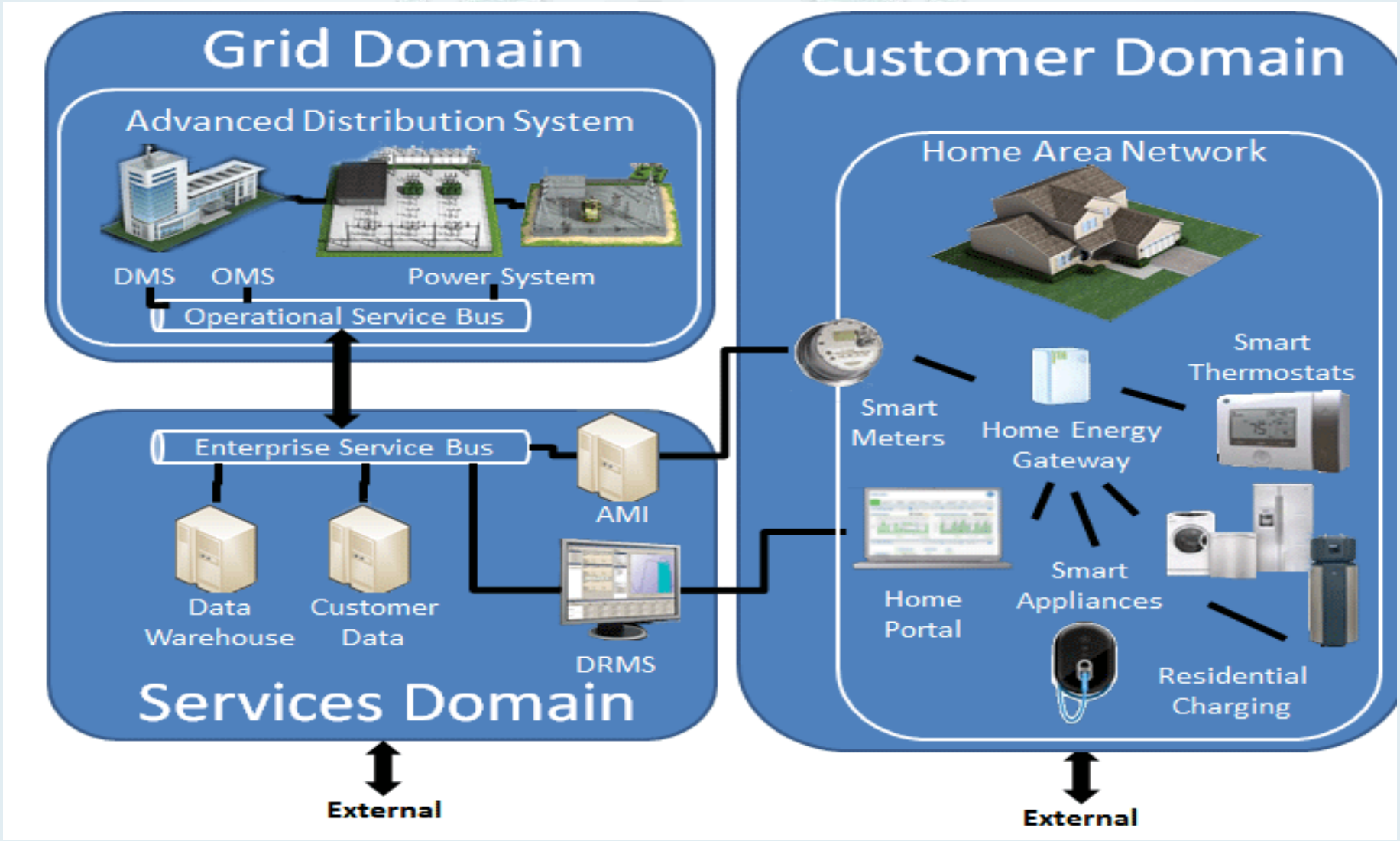
- Methodology for Operationalization;
- Operationalizing *Privacy by Design* across Smart Grid Domains;
- Working with partners – Hydro One, GE, IBM, Telvent.



www.privacybydesign.ca

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

Operationalizing *Privacy by Design* across Smart Grid Domains



Conclusions

- **Lead with *Privacy by Design;***
- **Change the paradigm from the dated "zero-sum" to the doubly-enabling "positive-sum;"**
- **Deliver *both* privacy AND security or any other functionality, in an empowering "win-win" paradigm;**
- **Embed privacy as a core functionality: the future of the Smart Grid may depend on it!**

How to Contact Us

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada

M4W 1A8

Phone: (416) 326-3948 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

For more information on *Privacy by Design*, please visit: www.privacybydesign.ca