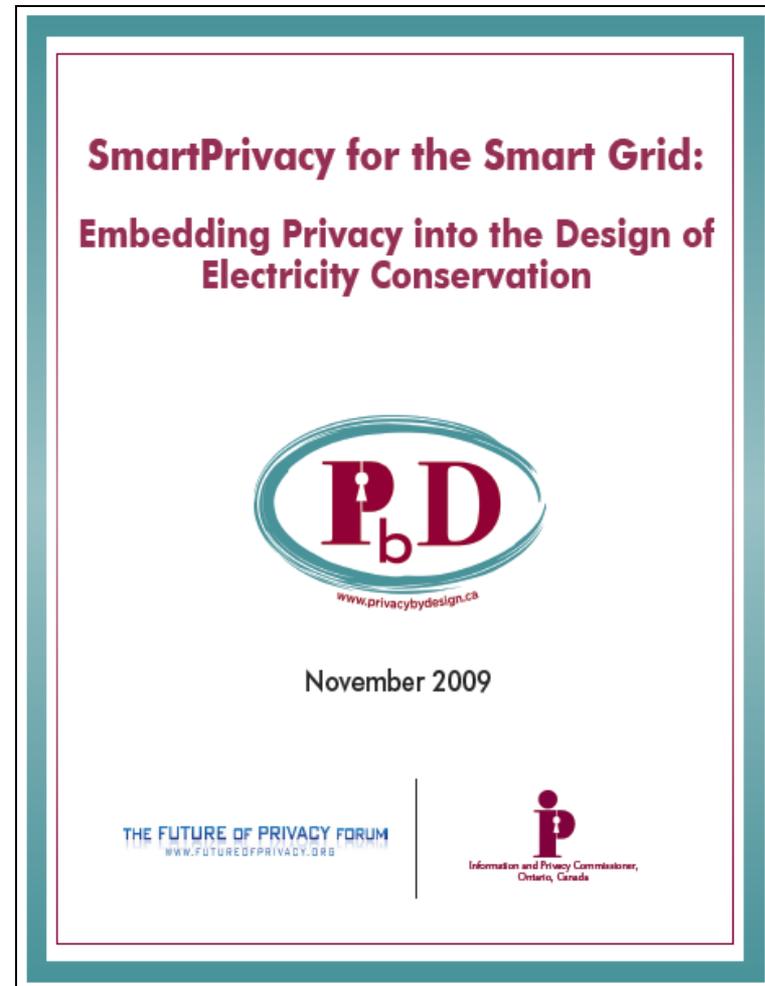


# **Privacy by Design and the Smart Grid**

## **SmartPrivacy for the Smart Grid: *Embedding Privacy into the Design of Electricity 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



## ***Privacy by Design in Smart Grid Guidance***

*“... this need to build privacy protections into systems and processes, along with the resulting benefits, is provided within the Privacy By Design methodology.”*

*National Institute of Standards and Technology, NISTIR 7628 Guidelines, Vol. 2.*

*“...the Privacy by Design methodology offers a promising approach to ensuring that data practices promote privacy, not just in the FIP of data minimization, but in all aspects of privacy planning.”*

*Decision 11-07-056, California Public Utility Commission, 2011*

*“The Smart Grids Task Force has agreed that a Privacy by Design approach is needed. This will be integrated in the standards being developed by the ESOs [European Standards Organizations].”*

*European Commission, April 12, 2011*

# ***Privacy by Design* in Smart Grid Guidance**

*“...**Security:** Cybersecurity and physical security should be provided to protect data, access points, and the overall electricity grid from unauthorized access and malicious attacks. **Privacy:** Respect and protect the privacy of customers. Integrate privacy requirements into smart grid planning and design from an early stage, including the completion of privacy impact assessments.”*

*Order-in-Council, Ontario Energy Board, November 2010*

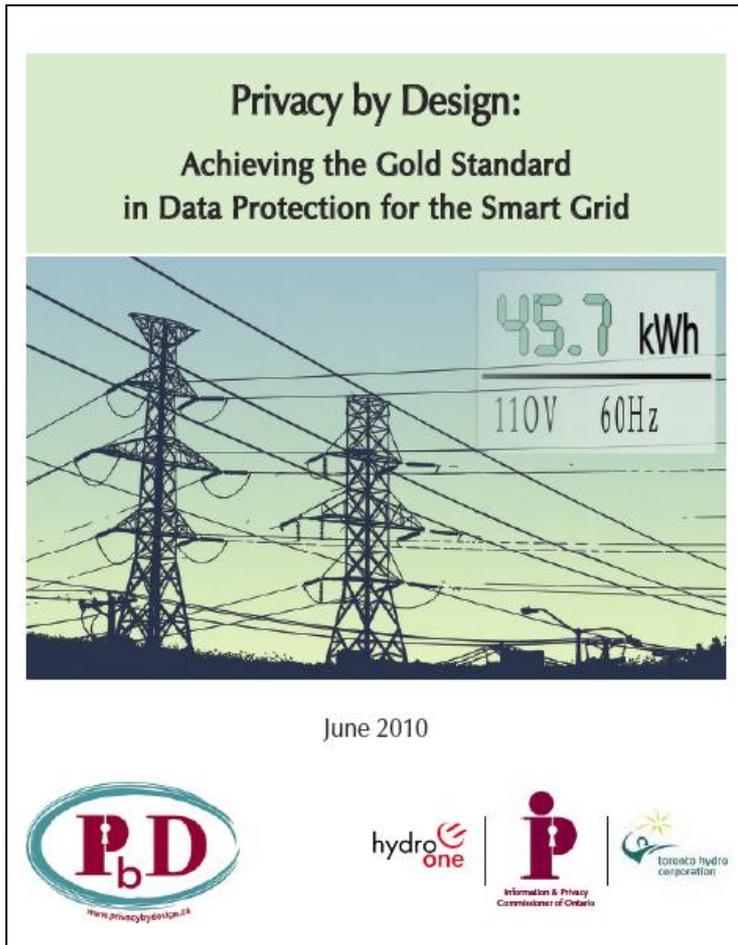
*“Recognizing that the seven Privacy by Design principles...provide valuable guidance with respect to compliance with applicable privacy laws...should be considered as best practice in implementation of the smart grid in Ontario for both regulated and unregulated service providers.”*

*Ontario Smart Grid Forum, 2<sup>nd</sup> report May 2011*

## Importance of Consumer Trust

- **California, USA:** Utilities installing smart meters faced blockades by homeowners, citing health and privacy concerns (2009/2010)
- **British Columbia, Canada:** Numerous citizen complaints spurred the B.C. Privacy Commissioner to launch an investigation of smart meter privacy (2012)
- **Netherlands:** Smart meter rollout halted due to public outcry about data privacy issues (2009)

# Hydro One (Canada)

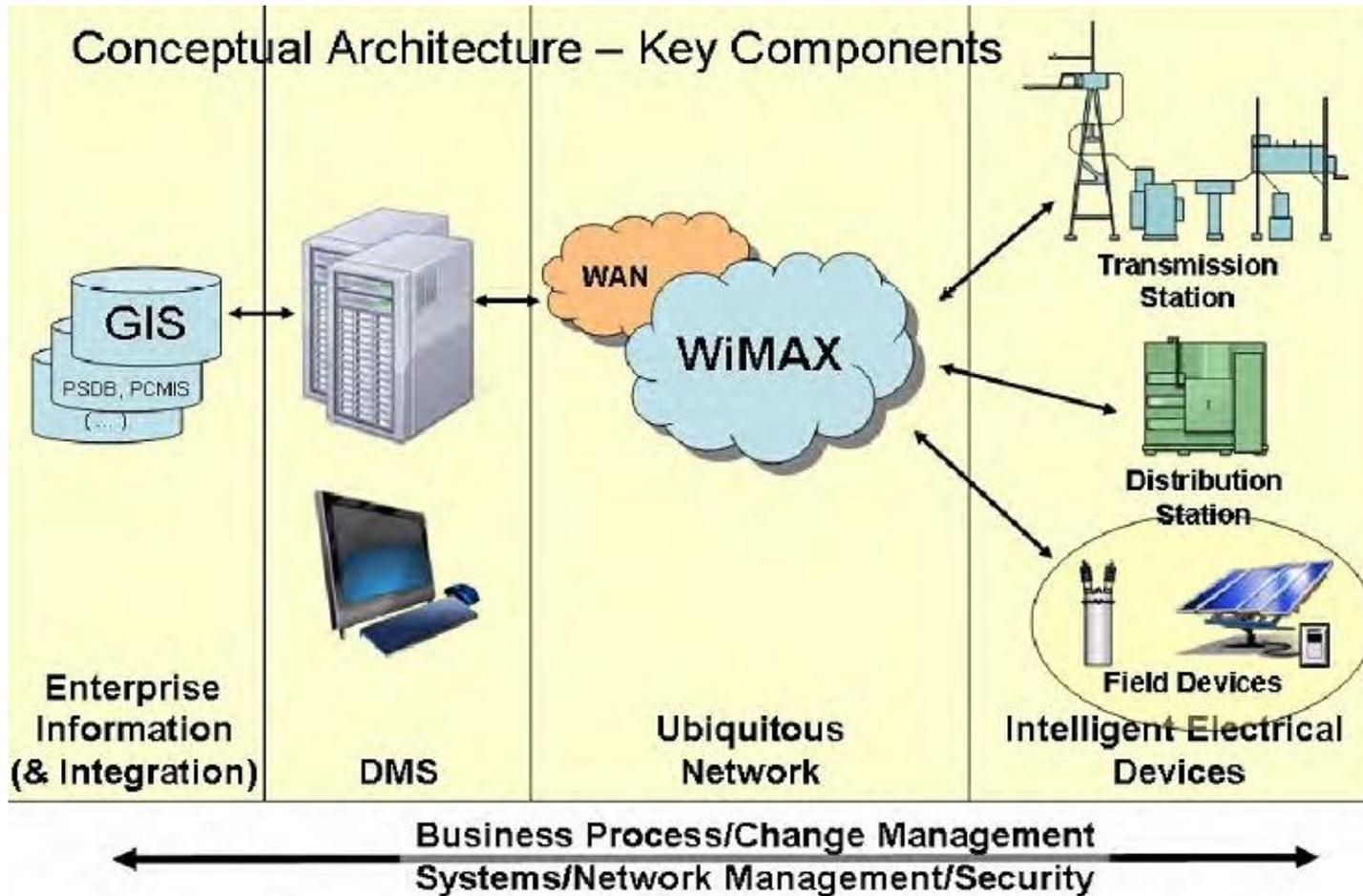


Methodology for Operationalization

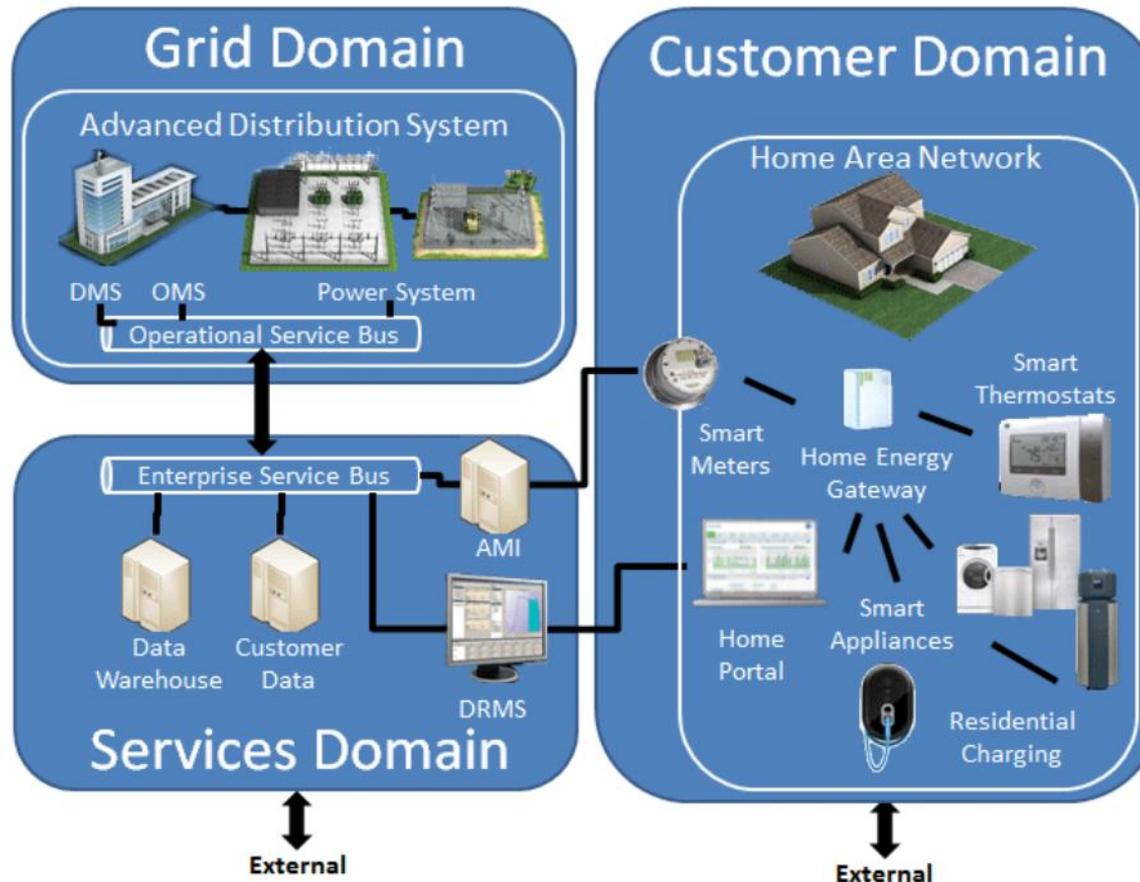
Operationalizing Privacy by Design across Smart Grid Domains

Working with partners – Hydro One, GE, IBM, Telvent.

# Architecture



# Operationalizing *Privacy by Design* across Smart Grid Domains



# SDG&E (USA)

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



March 2012



# Why Privacy?

- Perceptions of privacy continue to change
  - Paradigm-changing technologies like the Internet **impacted privacy** in ways we could have scarcely imagined 30 years ago
  - Today, Smart Grid technologies like smart meters are **changing the way we look at energy privacy**
- We know customers expect it
  - “SDG&E understands that the full benefits of Smart Grid **cannot be achieved** if it does not have the **confidence** of the users of the system.” (SGDP, pg. 139)

- It’s the **right thing to do**
- Regulators require it
  - CPUC Decision 11-07-056 – Electricity Usage Data Privacy Decision **applies strict rules** around how customer privacy is respected and protected
- Prudence demands it
  - Penalties for failure may be large

The CHRISTIAN SCIENCE  
**MONITOR**

## Sony data breach could be most expensive ever

Sony Corp.’s PlayStation Network and Sony Online Entertainment suffered data breaches that could cost up to \$2 billion.

By Mary Helen Miller, Correspondent / May 3, 2011

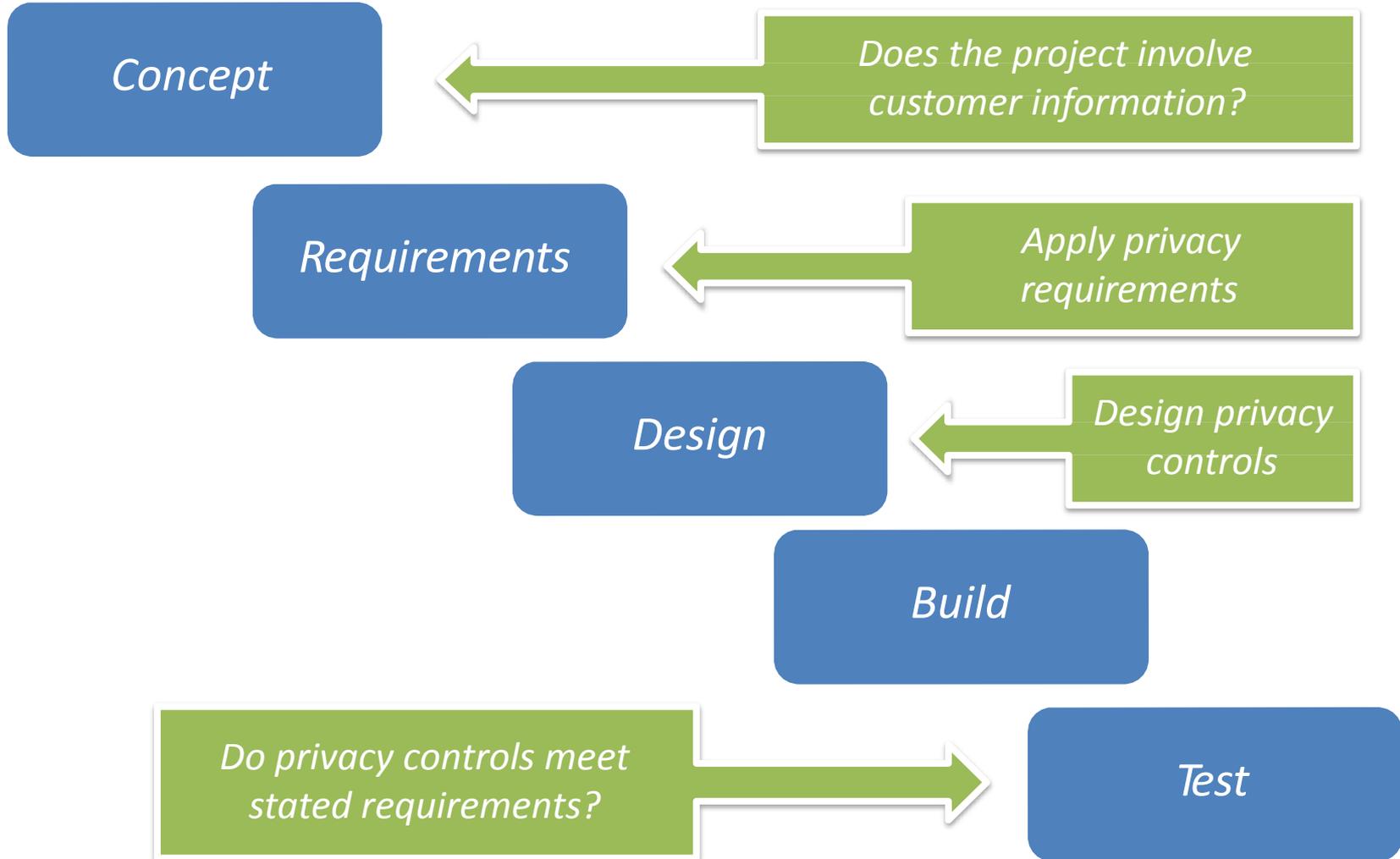
## ***Building a Privacy Program***

*While SDG&E has taken privacy seriously for over 100 years, in 2011 we began taking steps to formalize an **Office of Customer Privacy***

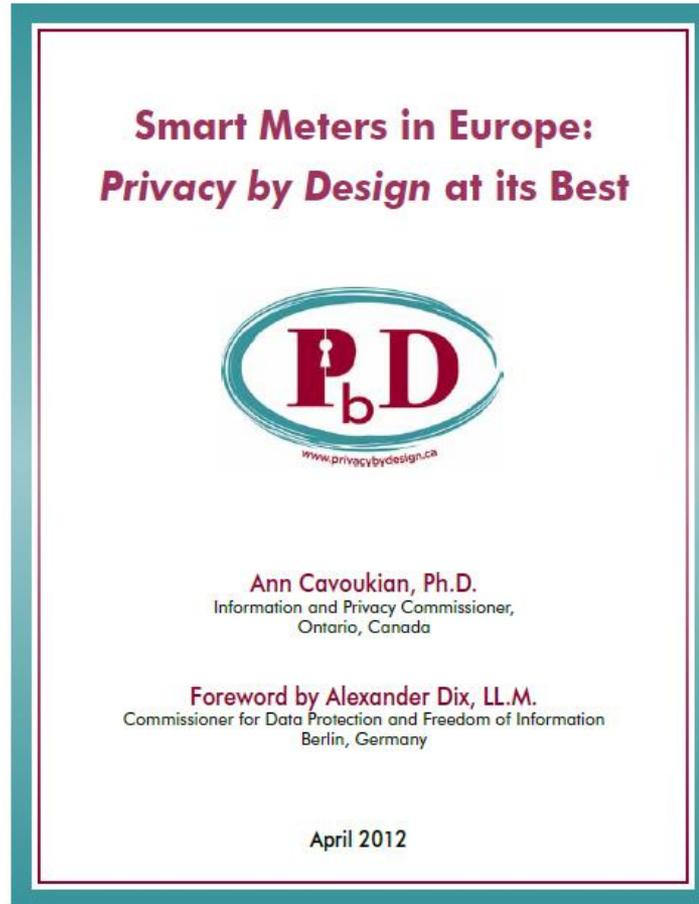
- *Developed Privacy Framework*
  - *Defines the "box", scopes how we look at privacy*
- *Developed a Privacy Impact Assessment*
  - *Allows employees to determine privacy risks related to changes*
- *Developed Privacy Controls*
  - *Provides mechanisms to ensure privacy is protected while information is collected, stored, handled, shared & disposed of*
- *Conduct Privacy Training*
  - *Role-based training to all company employees*
- *Raise Awareness*
  - *Engaging customers and third parties is CRITICAL to success!*
- *Engage Partners*
  - *Find subject matter experts to help improve the program over time*



# Privacy By Design Applied to Simplified IT Product Lifecycle



# Vatenfall Berlin (Europe)



## ***Vattenfall supports the energy efficiency program in Berlin-Maerkisches Viertel with installation of 10,000 smart meters.***

### ***Vattenfall's pilot project Maerkisches Viertel:***

- *Vattenfall installs 10,000 meters*
- *Leading technical development:*
  - *Mass test and PLC-test*
- *Energy saving contest increases customer involvement*
- *Customers can choose between different technologies. Customer response:*

### ***Berlin Maerkisches Viertel:***

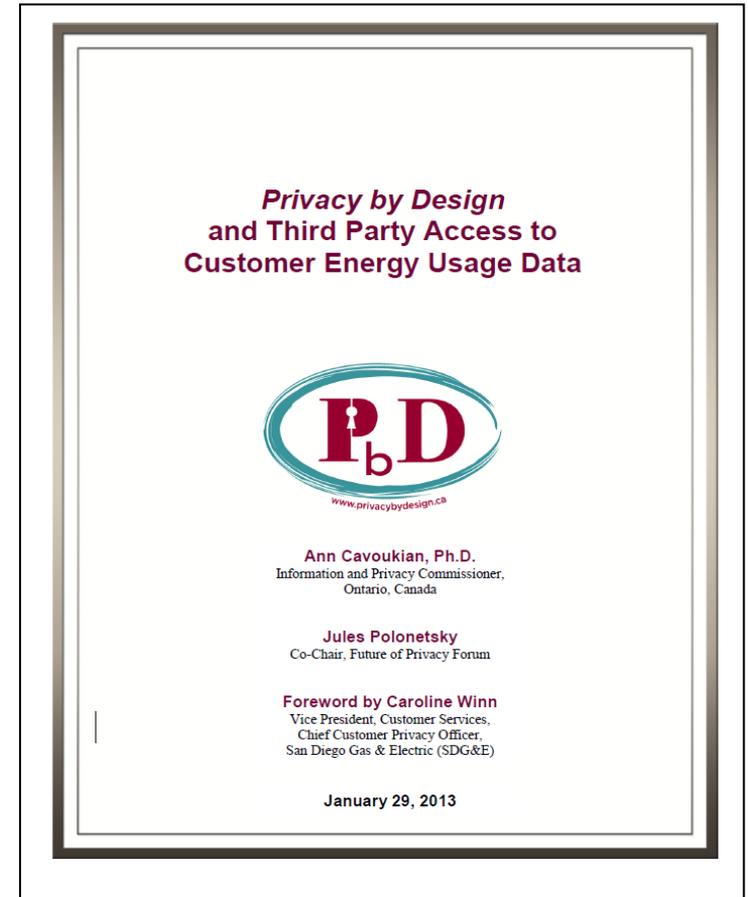
🕒 *More than 10,000 apartments with more than 50,000 inhabitants*

🕒 *Since 2007 award-winning energetical renovation of all apartments, ongoing*

- *EDL40 online visualization: ~900*
- *EDL21 TV visualization: ~350*
- *EDL21 basic visualization: ~8.750*



- Basic Data Flow Scenarios for Third Party Access to CEUD
  - Utility to Customer
  - Utility to Third Party
  - Device to Customer
- Examples of industry led approaches to privacy risks
  - Smart meter data aggregation protocols (Elster SG)
  - Analytics de-identification tool (Privacy Analytics Inc.)
  - Transparency and Consumer Education (Xcel Energy)
  - Privacy Seal (Future of Privacy Forum)
  - Green Button (MaRS Ontario, SDG&E)



- Integrate privacy into the development cycle of the app, and practice data minimization techniques;
- Even where there is permission from the user to access their data, must still ensure its proper and limited handling;
- Automatically limit the linking of additional data with personal information, and unlink when no longer required;
- Do not bury consent in a privacy policy;
- Avoid using mobile device identifiers or geo-location features as the default;
- When a customer requests their account deleted – delete it. Do not retain deleted accounts;
- etc.



# How to Contact Us

***Michelle Chibba, Director, Policy and Special Projects***

*Information and Privacy Commissioner's Office of 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](http://www.ipc.on.ca)*

*E-mail: [info@ipc.on.ca](mailto:info@ipc.on.ca)*