Practical Privacy by Design: Examples of Success

Ken Anderson
Assistant Commissioner (Privacy)
Ontario

Hong Kong
June 13, 2012

The Privacy Landscape

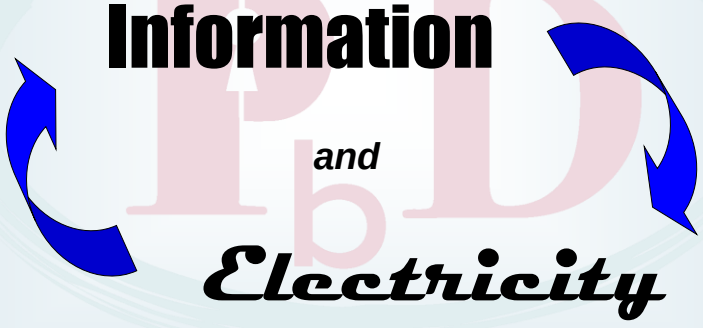
Privacy by Design in Action:

The Smart Grid

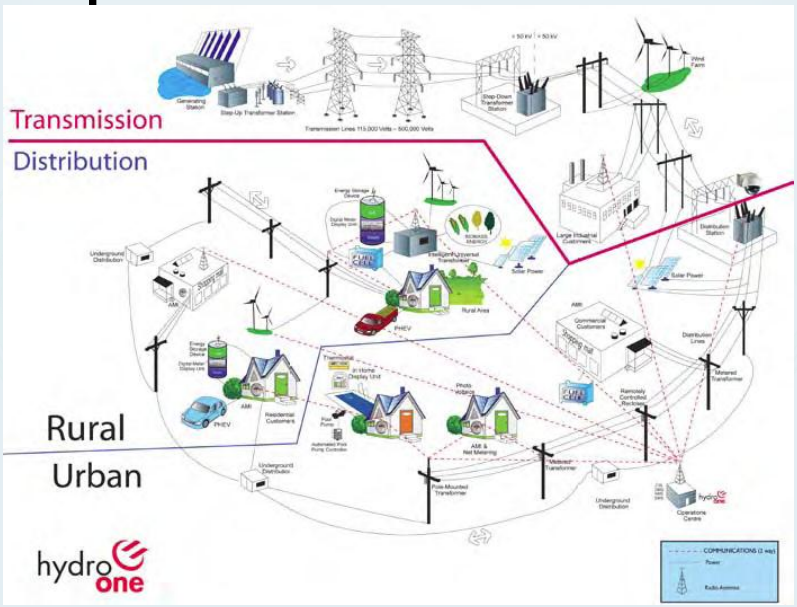
3

The Smart Grid: *What is it?*

A two-way flow of



Sample Smart Grid: Ontario



Imagining the Future: Elements of the Smart Grid

Smart Meters

Load Management

Smart Appliances

Dynamic Pricing

Access to Energy Information

Key Feature: Smart Meters

- Two-way connection between the utility and the home
- Records and reports **detailed** electricity consumption information ***automatically***
- Relays detailed information to the utility on a daily, hourly or ***real-time basis***

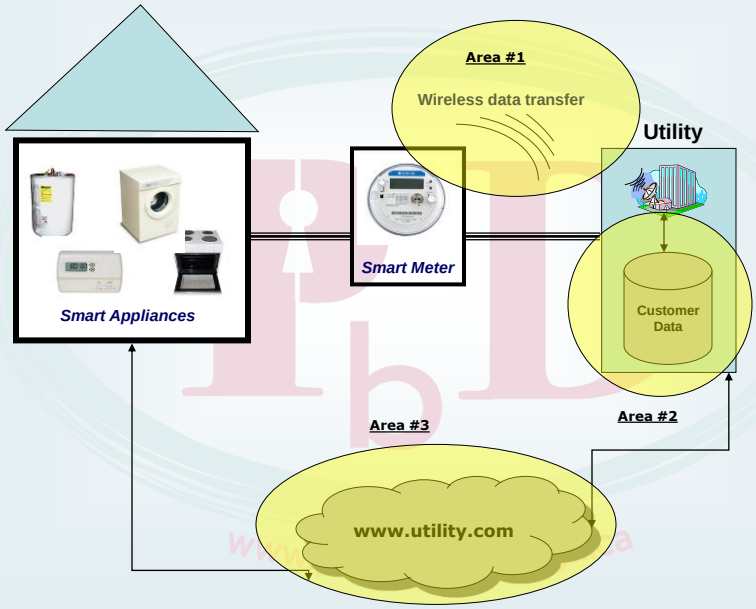
«

Key Feature: Dynamic Pricing

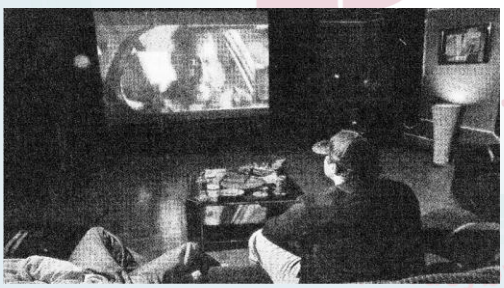
- ***Time-of-use pricing:*** Energy prices are higher at pre-designated peak times and lower at others
- ***Critical peak pricing:*** Where the rate is set much higher for the most critical peak hours
- ***Real-time pricing:*** Where prices vary by the hour according the utility's cost to purchase or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

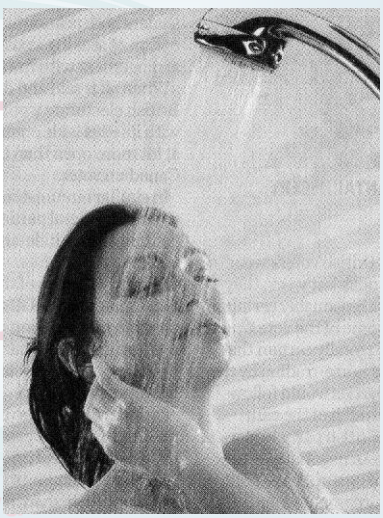
»

Key Privacy Risk Areas



Can the Smart Grid Know Too Much?





10

Images – Toronto Star/Shutterstock – May 12, 2010

Personally Identifiable Information and the Smart Grid

- Modernization of the current electrical grid will involve end-user components and activities that will lead to increasing the collection, use and disclosure of personal information by utility providers, as well as third-parties
- What constitutes "personal information" on the Smart Grid is the subject of much discussion
- In the context of the Smart Grid, the linkage of any personally identifiable information with energy use would render the linked data as personal information and privacy considerations immediately apply

11

Smart Grid: Privacy Risks

- An electricity usage profile can translate into a source of detailed behavioural information
- Digital data is vulnerable to unauthorized access, copying, matching, merging and widespread dissemination for secondary purposes without the consent of the consumer

12

Personal Privacy Must Remain Paramount

"So far, Ontario is the leading the game, but the modernization of the grid is in its infancy and if vigilance isn't maintained, personal habits could become everyone's business."

— Commissioner Cavoukian

"We've taken the advice of the privacy commissioner upfront before the smart grid is even put in place."

— Brad Duguid, Ontario Minister of Energy and Infrastructure

***Toronto Star*, May 12, 2010**

CANADA

Can smart grid know too much?

Hydro meter info a boon for thieves, marketers, and must be protected, privacy czar says

THEY KNOW WHEN YOU ARE SLEEPING ...

THEY KNOW WHEN YOU'RE IN THE SHOWER

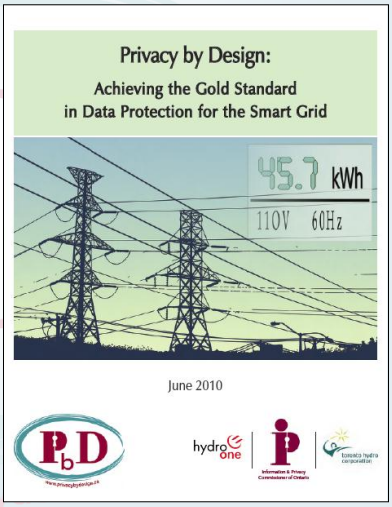
THEY KNOW WHEN YOU'RE AWAKE ...

What time you sleep, cook, shower, turn on the TV, or set the alarm system can be tracked by the province's emerging smart-grid hydro system, possibly tipping off thieves to a household's habits. "This thing has to be protected like Fort Knox," says Ontario's privacy commissioner Ann Cavoukian.

http://tinyurl.com/24dzn9j

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.ipc.on.ca

Identity, Privacy and Security Institute
University of Toronto

IPSI is dedicated to developing new approaches to security that maintain the privacy, freedom and safety of the individual and the broader community

Engineering – Mathematics – Computer Sciences – Information Studies

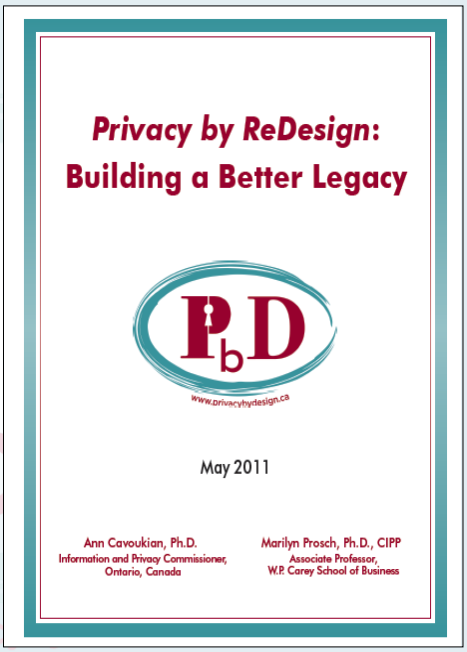
www.ipsi.utoronto.ca

15

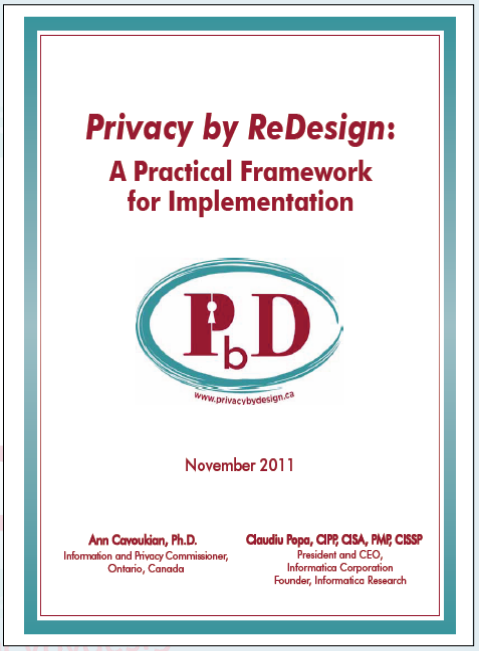
Privacy by *Re*Design
PbRD

16

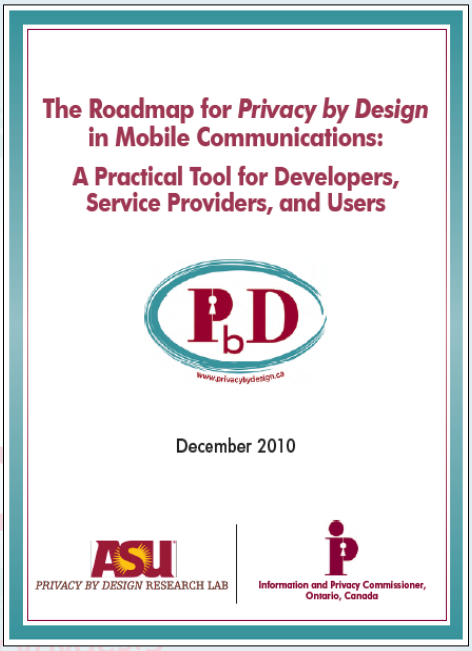
1. ***Rethink:*** review existing risk mitigation strategies and systems, considering alternatives that will be more privacy protective;
2. ***ReDesign:*** develop and enable improvements in the system that will deliver original function and privacy in a doubly-enabling, positive-sum manner;
3. ***Revive:*** re-launch the newly improved, more privacy protective system.



- Identifying potential targets for *Privacy by ReDesign*;
- Practical framework for implementing *Privacy by ReDesign*;
- Laying the foundations for success;
- A road map towards proactive data protection.

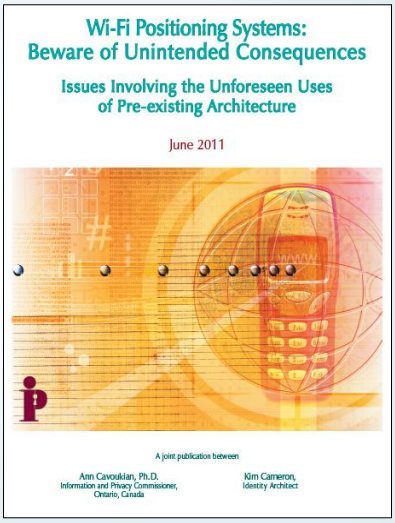


- Widespread Adoption of Mobile Communications Technology;
- Privacy and Mobile Communications;
- Roadmap for *PbD* in the Mobile Communications Industry:
  - Device Manufacturers;
  - OS/Platform & Application Developers;
  - Network Providers.



Wi-Fi Positioning Systems: Beware of Unintended Consequences

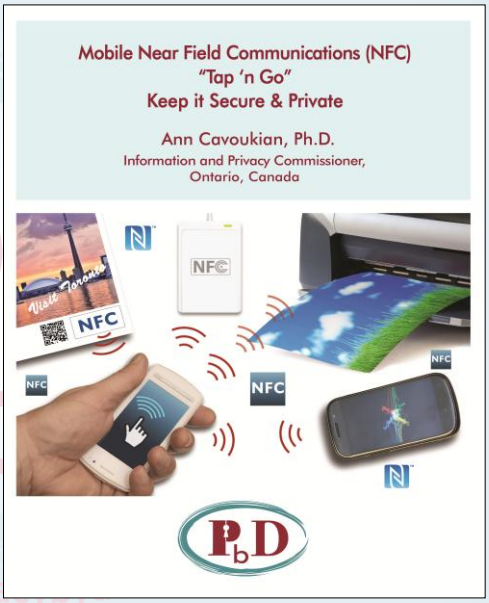
- Advances in location-based technology and services;
- Overview of major positioning systems;
- Wi-Fi Positioning System "location aggregators;"
- *Privacy by Design*: Removing the "Informant" from WPS Location Architecture.



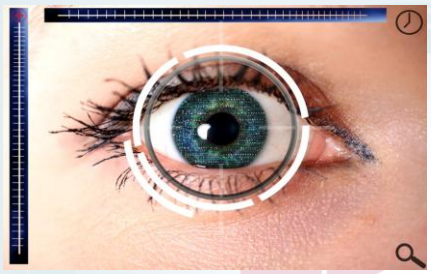
www.privacybydesign.ca

Near Field Communications (NFC) White Paper

- Residual security and privacy risks;
- NFC use cases;
- *Privacy by Design* to mitigate risks;
- Infrastructures of ubiquitous surveillance are emerging – must be mitigated.



Biometric Encryption



www.ipc.on.ca/images/Resources/untraceable-bio.pdf

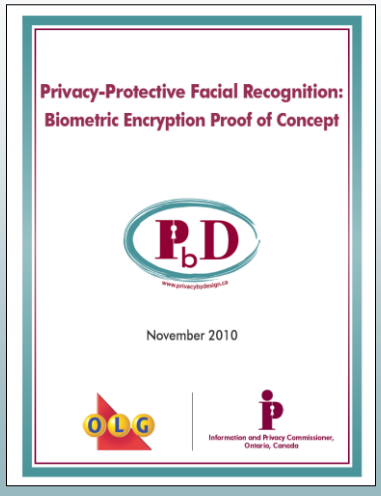
Biometric Encryption (BE)

What is Biometric Encryption?

- Class of emerging "untraceable biometrics" technologies that seek to translate the biometric data provided by the user;
- Special properties:
  - uniqueness
  - irreversibility

Facial Recognition: *Biometric Encryption Approach*

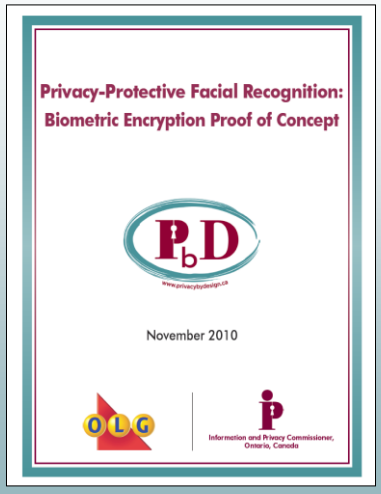
"The rapid, accurate identification and authentication of individuals has become a challenge across many sectors and jurisdictions … Increasingly, biometric encryption is being viewed as the ultimate means of authentication or identification across a broad range of applications."



www.privacybydesign.ca

Facial Recognition: *Biometric Encryption Approach*

"The rapid, accurate identification and authentication of individuals has become a challenge across many sectors and jurisdictions … Increasingly, biometric encryption is being viewed as the ultimate means of authentication or identification across a broad range of applications."



www.privacybydesign.ca

OLG Facial Recognition Program

- The system is designed to detect only self-excluded people – not cheaters or organized crime;
- Legacy, photograph-based system, needs to be maintained without the need for re-enrolment of individuals;
- Automated facial recognition system is the only technology that produces remote identification and is compatible with the legacy photograph-based system.

Facial Recognition with Biometric Encryption

- ***Biometric Encryption*** (BE): securely binds a person's identifier (pointer to personal information) with facial biometrics;
- The pointer is retrieved only if a correct (i.e., self-excluded) person is present;
- The link between facial templates and personal information is controlled by BE;
- Final comparison is done manually;
- Privacy of both the general public ***and*** self-excluded individuals is protected.

Proof of Concept

- Live field test at Woodbine facilities: Correct Identification Rate (CIR) is 91% without BE, and 90% with BE – negligible accuracy impact;
- BE reduces False Acceptance Rate (FAR) by up to 50% – a huge improvement in accuracy;
- Accuracy exceeds state-of-the-art for facial recognition;
- ***Triple-win***: privacy, security, and accuracy (unexpected) – all improved;
- **Next:** production version of facial recognition with BE.

Fostering Privacy and Innovation at MaRS

beringmedia

CognoVision
Intelligent. Imaging. Analysis.

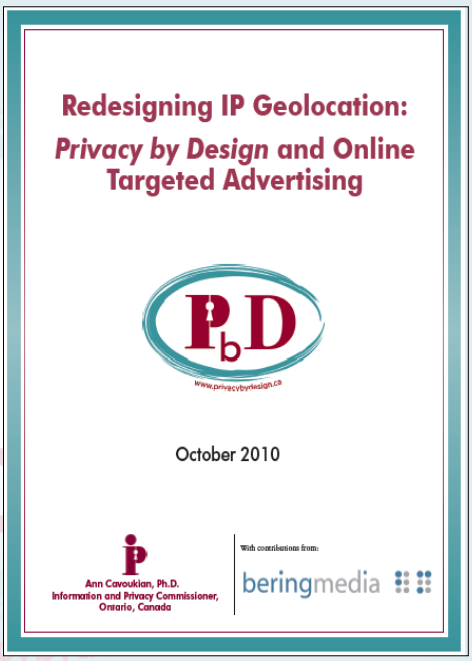
Connected n
simply connected

PrivIT | Healthcare

SKYMETER

29

- **Bering Media** has built Privacy into IP Geolocation:
- Using a unique double-blind privacy architecture;
- With minimum-match thresholds/ Anti-inference algorithms;
- Dynamic IP address management;
- Persistent, permanent opt-out.



www.ipc.on.ca/images/Resources/pbd-ip-geo.pdf

30

The Next Evolution in Data Protection:

"SmartData"

Developed at IPSI, *SmartData* represents the future of privacy and the control of personal information online

Intelligent or "smart agents" introduced into IT systems virtually – thereby creating "*SmartData,*" – a new approach to Artificial Intelligence that will revolutionize the field.

www.ipc.on.ca/images/Resources/bio-encrypt-chp.pdf

Conclusions

- **Lead with *Privacy by Design***
- **Change the paradigm from "zero-sum" to "positive-sum"**
- **Deliver *both* privacy AND security in a doubly enabling "win-win" paradigm**
- **Embed privacy as a core functionality: the future of privacy will depend on it!**

Appendix

- The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices (http://www.privacybydesign.ca/papers.htm)
- *Privacy by Design*: Achieving the Gold Standard in Data Protection for the Smart Grid (http://www.ipc.on.ca/images/Resources/achieve-goldstnd.pdf)
- Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security *AND* Privacy (*http://www.ipc.on.ca/index.asp?navid=46&fid1=608*)
- Wireless Communications Technologies: Video Surveillance Systems (*http://www.ipc.on.ca/index.asp?navid=46&fid1=626*)
- Fingerprint Biometrics: Address Privacy Before Deployment (*http://www.ipc.on.ca/index.asp?navid=46&fid1=816*)
- Fingerprint Biometric Systems: Ask the Right Questions Before You Deploy (*http://www.ipc.on.ca/index.asp?navid=46&fid1=769*)
- Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum (*http://www.ipc.on.ca/index.asp?navid=46&fid1=758*)
- Practical Tips for Implementing RFID Privacy Guidelines (*http://www.ipc.on.ca/index.asp?navid=46&fid1=430*)
- Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report - Privacy Investigation (*http://www.ipc.on.ca/index.asp?navid=53&fid1=7874*)
- Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines) (*http://www.ipc.on.ca/index.asp?navid=46&fid1=432*)
- RFID and Privacy: Guidance for Health-Care Providers (*http://www.ipc.on.ca/index.asp?navid=46&fid1=724*)
- What's New Again? Security Measures Must Be Real – Not Illusory (*http://www.ipc.on.ca/index.asp?navid=46&fid1=813*)
- The Relevance of Untraceable Biometrics and Biometric Encryption: A Discussion of Biometrics for Authentication Purposes (*http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=879*)
- Whole Body Imaging in Airport Scanners: Building in Privacy by Design (*http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=846*)
- Privacy by Design ... Take the Challenge *(http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=856)*

Conclusions

- **Lead with *Privacy by Design***
- **Change the paradigm from "zero-sum" to "positive-sum"**
- **Deliver *both* privacy AND security in a doubly enabling "win-win" paradigm**
- **Embed privacy as a core functionality: the future of privacy will depend on it!**

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

35