Getting Smart About Privacy on the Smart Grid

Ken Anderson

Assistant Commissioner, Privacy

Ontario, Canada

Osgoode Professional Development
Toronto, Ontario
April 7, 2010

Who We Are

Commissioner Ann Cavoukian, Ph.D.

- appointed by Ontario legislature
- independent from government
- oversees 3 privacy & access to information laws

Mandated to:

- investigate privacy complaints
- resolve appeals from refusals to provide access to information
- ensure organizations comply with access and privacy provisions of the *Acts*
- educate public about Ontario's access and privacy laws
- conduct research on access and privacy issues, provide advice and comment on proposed government legislation & programs.

Key Definitions

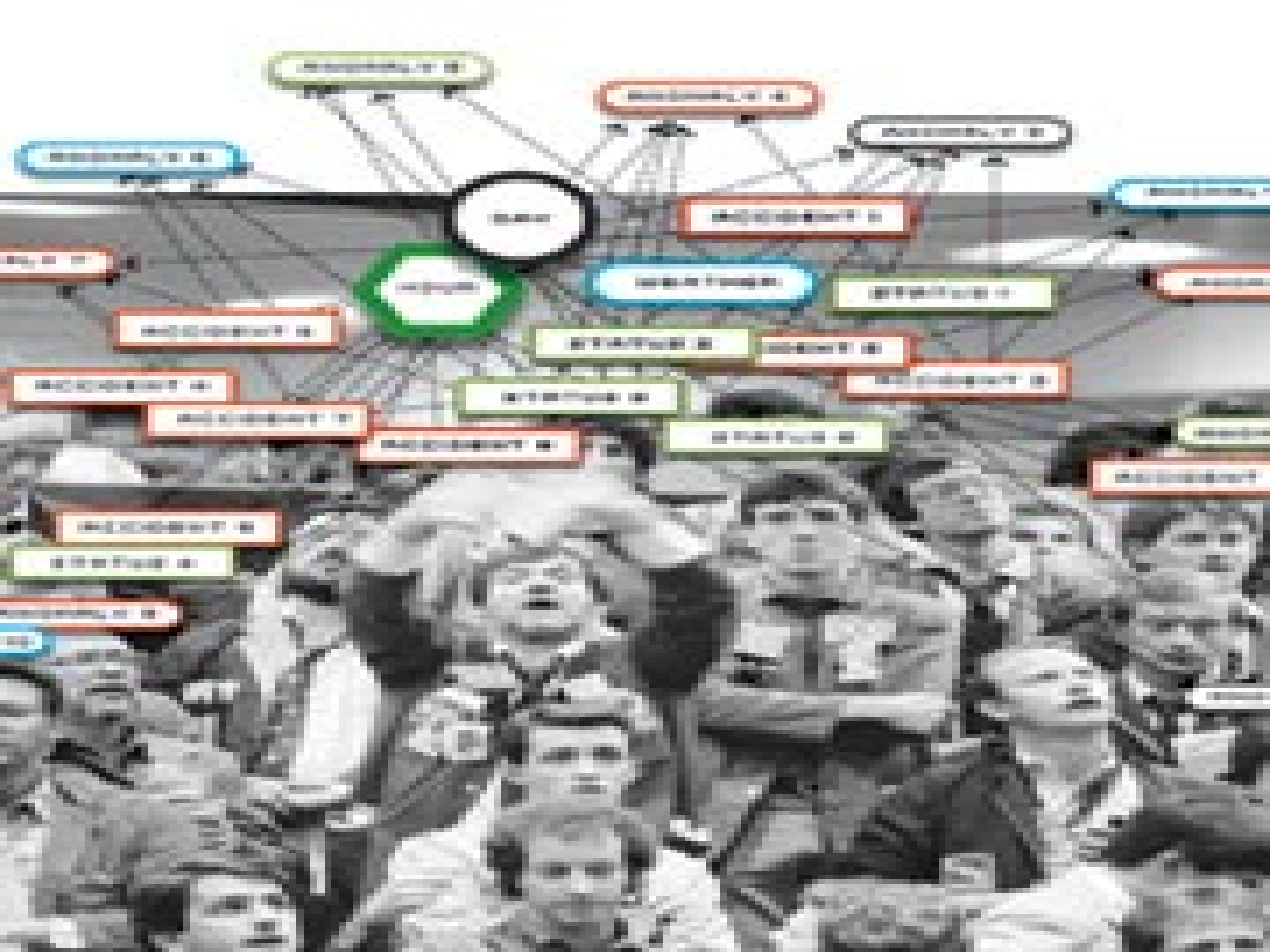
- **Information privacy** refers to the right or ability of individuals to exercise control over the collection, use and disclosure by others of their personal information
- **Personally-identifiable information ("PII")** can be biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational or reputational, and is the stuff that makes up our modern identity

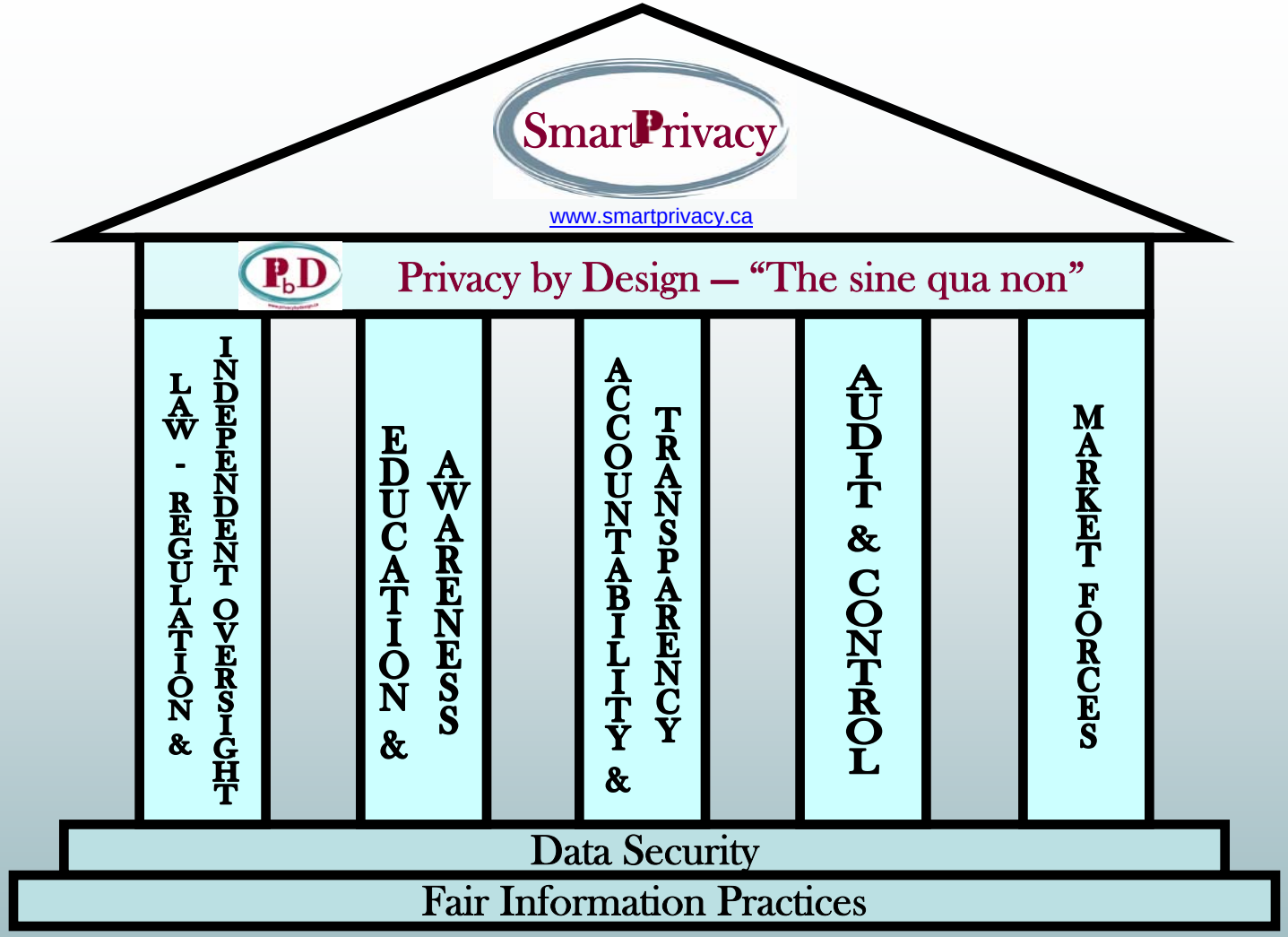
Personal information must be managed responsibly. When it is not, accountability is undermined and confidence in our evolving information society is eroded.

What Privacy is Not

Privacy ≠ Security

Security *is*, however, vital to privacy





"SmartPrivacy is the umbrella that offers the complete suite of protections to ensure data privacy. It consists of multiple measures ranging from regulatory protections to education and awareness, but one measure stands out as the sine qua non: *Privacy by Design*. *Dr. Ann Cavoukian, Information & Privacy Commissioner of Ontario, Canada, August 13, 2009.*

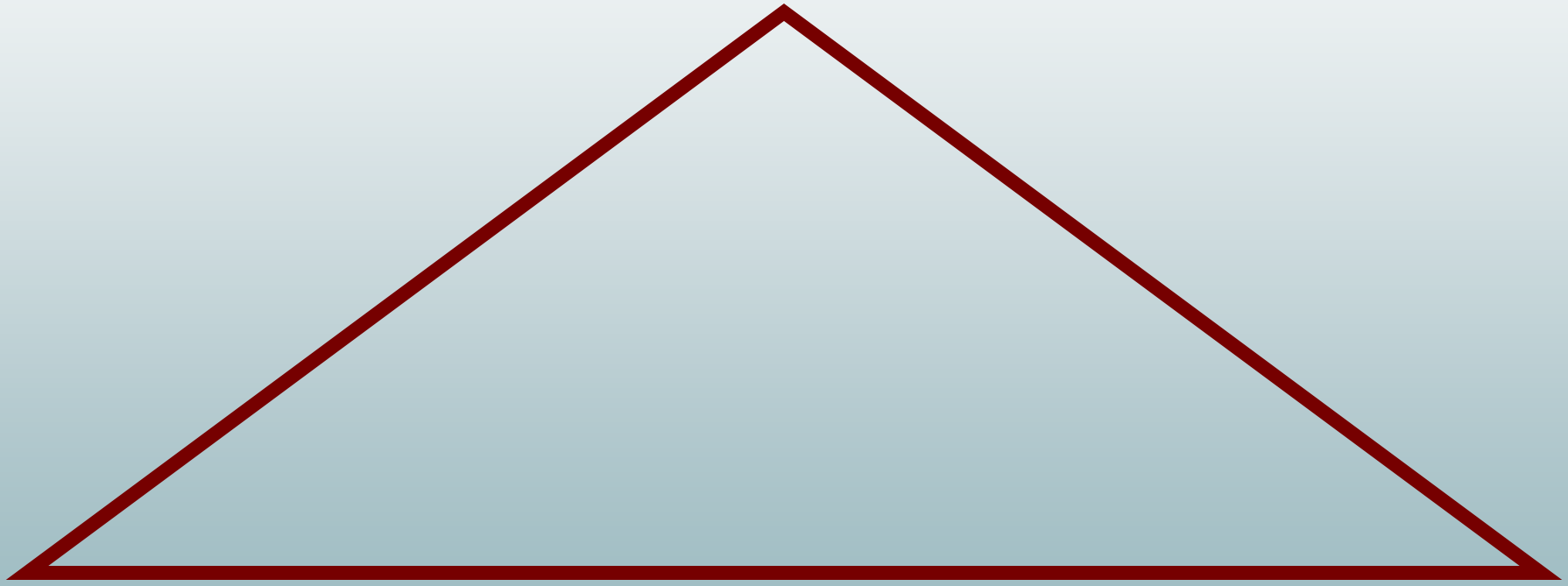
SmartPrivacy Foundations v1.0


PbD
www.privacybydesign.ca

***Privacy by Design*: "Build It In"**

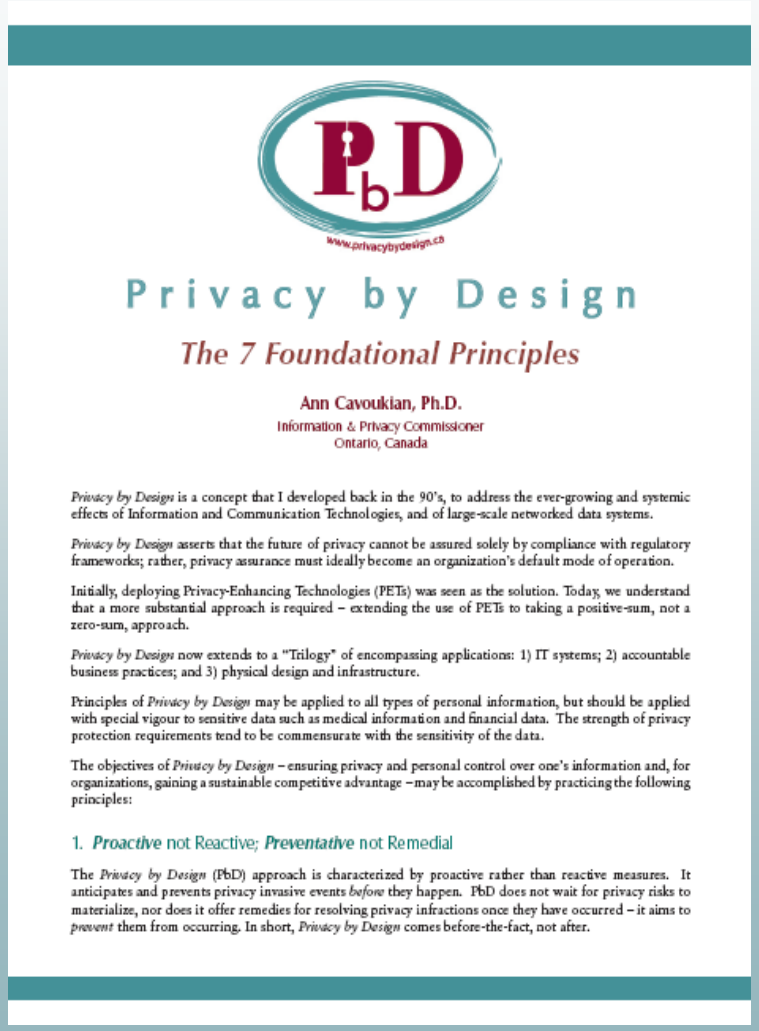
- The Commissioner first developed the concept of ***Privacy by Design*** in the 90s, as a response to the growing threats to online privacy that were beginning to emerge;
- ***Privacy by Design* seeks to build in privacy** – up front, right into the design specifications; into the architecture; embed privacy into the technology used – ***bake it in***;
- **Data minimization is key**: minimize the routine collection and use of personally identifiable information – use encrypted or coded information whenever possible;
- **Use PETs *Plus*** (positive-sum, not zero-sum) wherever possible: give people maximum control over their own data.

Privacy by Design:
The Trilogy of Applications



Privacy by Design:
The 7 Foundational Principles

1. *Proactive* not Reactive;
   Preventative not Remedial
2. Privacy as the *Default*
3. Privacy E*mbedded* into Design
4. *Full* Functionality:
   Positive-Sum, not Zero-Sum
5. End-to-End Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy



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 that 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 asserts 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 understand that a more substantial approach is required – extending the use of PETs to taking a positive-sum, not a zero-sum, approach.

Privacy by Design now extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and 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 protection requirements tend to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* – ensuring privacy and personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the following principles:

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

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

Why We Need *Privacy by Design*

- Most privacy breaches remain undetected – as regulators, we only see the tip of the iceberg;
- The majority of privacy breaches remain unchallenged, unregulated ... unknown;
- Compliance alone, is unsustainable as the sole model for ensuring the future of privacy; for that, we must turn to proactive measures such as ***Privacy by Design:*** embedding privacy *proactively* into the core of all that we do.

Applying Privacy to Information Systems

- **Minimize collection, use, sharing, and retention of PII**
  (*e.g.*, limiting purposes, collection, use, disclosure, and retention)
- **Enhance data security**
  (*e.g.*, appropriate safeguards)
- **Actively engage the individual in managing and controlling their PII**
  (*e.g.*, consent, accuracy, access, challenging compliance, etc.)

SmartPrivacy for the Smart Grid

Smart Grid Goals

- Consumer choice of how, when, quantity
- Self-heal in case of disturbance/attacks
- Link with array of energy sources
- Improved energy quality & efficiency

Smart Grid Qualities

- Intelligent – self-sensing
- Efficient – no/little new infrastructure
- Accommodating – accepts many sources
- Motivating – enables choice/incentives
- Opportunistic – fosters new innovation
- Quality-focused – no sags, spikes, disturbance
- Resilient – resists attacks or disasters - decentralized
- “Green” – provides environmental improvement

Grid Structure

- Smart Meters
- Smart Appliances
- Dynamic Pricing
- Tracking & Monitoring Tools
- Load Management Technologies

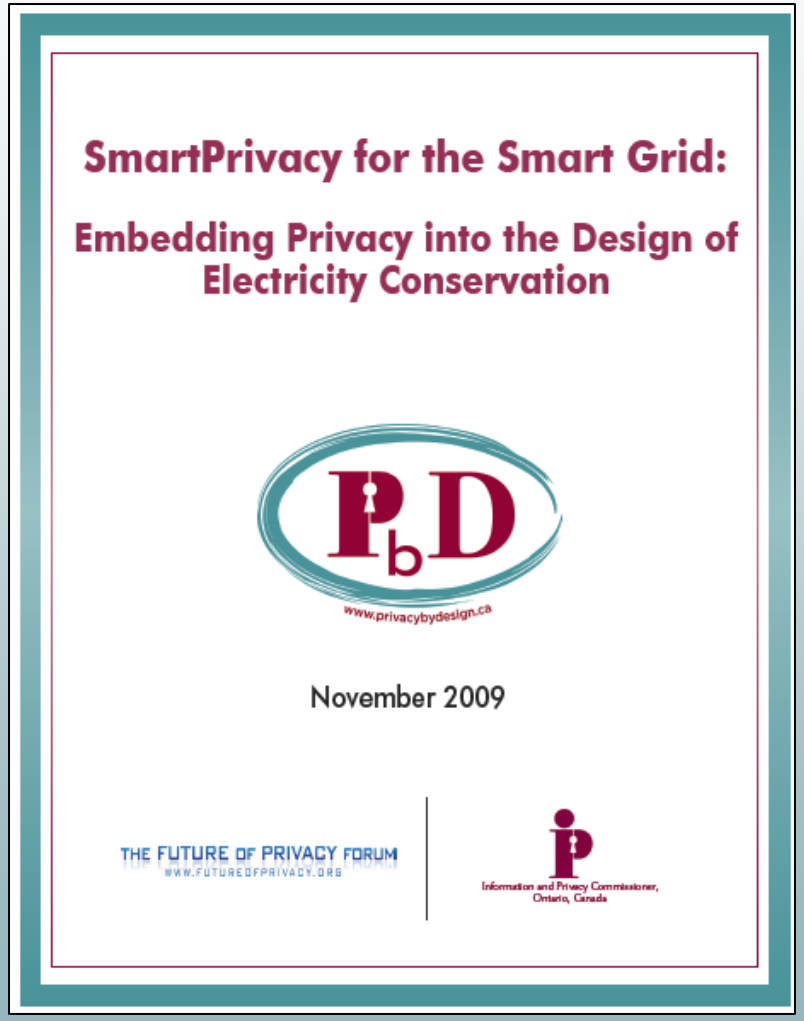
Personal Information Tracked?

- Personal Habits
- Behaviours
- Lifestyles

SmartPrivacy for the Smart Grid: A Case in Point

"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's not top-of-mind."

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

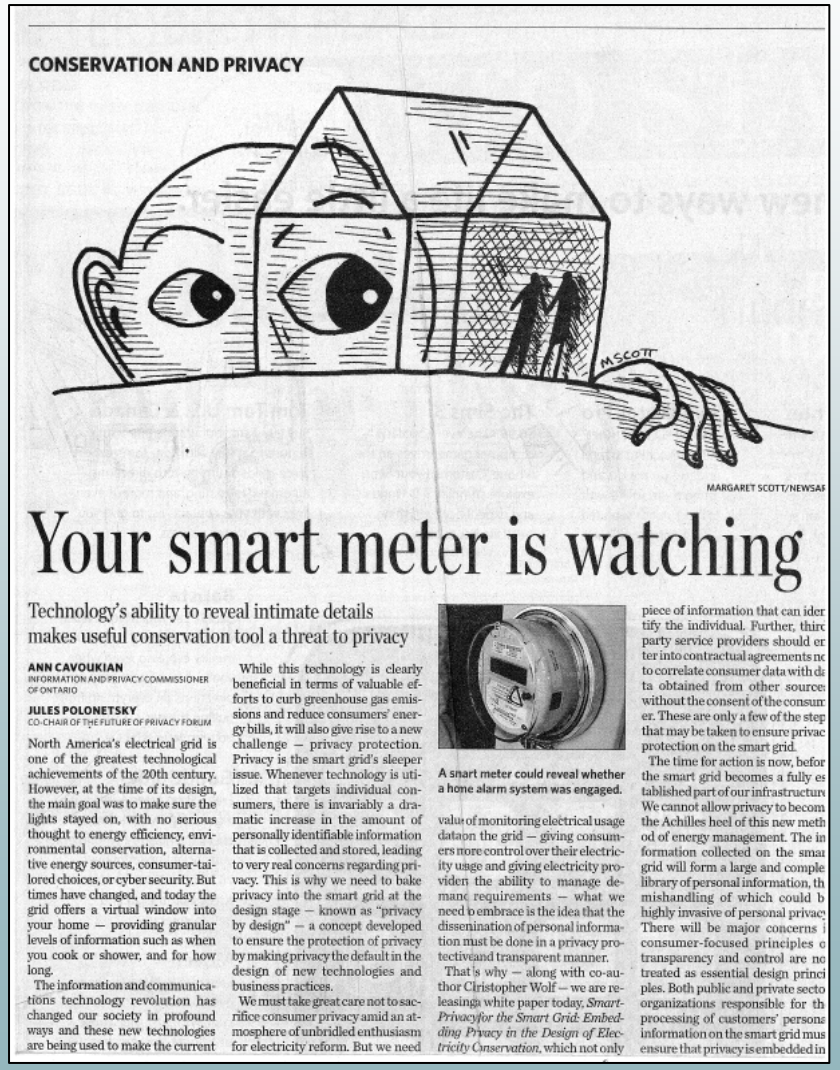


www.privacybydesign.ca

Commissioner Cavoukian's Op-Ed, with Jules Polonetsky, Future of Privacy Forum:

Toronto Star
Tuesday, November 17, 2009

"Privacy is the smart grid's sleeper issue. Whenever technology is utilized that targets individual consumers, there is invariably a dramatic increase in the amount of personally identifiable information that is collected and stored, leading to very real concerns regarding privacy …the time for action is now, before the smart grid becomes a fully established part of our infrastructure. We cannot allow privacy to become the Achilles heel of this new method of energy management." – p.A27



CONSERVATION AND PRIVACY

MARGARET SCOTT/NEWSAG

Your smart meter is watching

Technology's ability to reveal intimate details makes useful conservation tool a threat to privacy

ANN CAVOUKIAN
INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

JULES POLONETSKY
CO-CHAIR OF THE FUTURE OF PRIVACY FORUM

North America's electrical grid is one of the greatest technological achievements of the 20th century. However, at the time of its design, the main goal was to make sure the lights stayed on, with no serious thought to energy efficiency, environmental conservation, alternative energy sources, consumer-tailored choices, or cyber security. But times have changed, and today the grid offers a virtual window into your home – providing granular levels of information such as when you cook or shower, and for how long.

The information and communications technology revolution has changed our society in profound ways and these new technologies are being used to make the current

While this technology is clearly beneficial in terms of valuable efforts to curb greenhouse gas emissions and reduce consumers' energy bills, it will also give rise to a new challenge – privacy protection. Privacy is the smart grid's sleeper issue. Whenever technology is utilized that targets individual consumers, there is invariably a dramatic increase in the amount of personally identifiable information that is collected and stored, leading to very real concerns regarding privacy. This is why we need to bake privacy into the smart grid at the design stage – known as "privacy by design" – a concept developed to ensure the protection of privacy by making privacy the default in the design of new technologies and business practices.

We must take great care not to sacrifice consumer privacy amid an atmosphere of unbridled enthusiasm for electricity reform. But we need

A smart meter could reveal whether a home alarm system was engaged.

value of monitoring electrical usage data on the grid – giving consumers more control over their electricity usage and giving electricity providers the ability to manage demand requirements – what we need to embrace is the idea that the dissemination of personal information must be done in a privacy protective and transparent manner.

That is why – along with co-author Christopher Wolf – we are releasing a white paper today, *Smart Privacy for the Smart Grid: Embedding Privacy in the Design of Electricity Conservation*, which not only

piece of information that can ider tify the individual. Further, thirc party service providers should er ter into contractual agreements nc to correlate consumer data with da ta obtained from other sources without the consent of the consum er. These are only a few of the step that may be taken to ensure privac protection on the smart grid.

The time for action is now, befor the smart grid becomes a fully es tablished part of our infrastructure We cannot allow privacy to becom the Achilles heel of this new meth od of energy management. The in formation collected on the sma grid will form a large and comple library of personal information, th mishandling of which could b highly invasive of personal privacy There will be major concerns i consumer-focused principles o transparency and control are nc treated as essential design princi ples. Both public and private secto organizations responsible for th processing of customers' persona information on the smart grid mus ensure that privacy is embedded in

www.thestar.com/comment/article/726528

Smart Grid:
Privacy Risks

- 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;
- 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;
- The information collected on a smart grid can form a library of personal information, the mishandling of which can lead to invasions of consumer privacy;
- An electricity usage profile can translate into a source of detailed behavioural information;
- Major concerns will arise if consumer-focused principles of transparency and control are not treated as essential design principles, from end to end, throughout the entire data lifecycle.


PREV SEAS
RATE ABCD
CONT CUM
RESETS MAX
TOTAL KVARh
A B C
LOCK
RESET
CL200, 120 TO 480V, 4WY or 4WD, 60Hz
FM 16S (15S, 14S) Watthour Meter
Kh 21.6
P/R 24

Smart Grid:*Our Position*

- While the smart grid is a positive undertaking, the focus has almost exclusively been on controlling energy use, thereby making privacy a sleeper issue;
- We must ensure that consumer privacy is not sacrificed amidst a sea of unbridled enthusiasm for electricity reform – we must insist upon a positive-sum, ***not*** a zero-sum approach;
- Principles of *Privacy by Design* must form part of the overall design for Smart Grid data flows.

Smart Grid With SmartPrivacy

Maintain full functionality AND:

- Intelligent – collect minimum personal information
- Efficient – no privacy/security compromise
- Accommodating – consumer preferences easily accepted
- Motivating – communicate notice & obtain prior consent
- Opportunistic – foster privacy-enhancing technologies
- Quality-focused – personal information maintained is accurate + accessible
- Resilient – resists data breaches
- “Green” – consumer trust can increase participation

IPC Outreach Regarding Smart Grid

- Ontario Ministry of Energy and Infrastructure;
- Ontario Energy Board;
- Joint meeting in Washington D.C. with Gridwise Alliance and Future of Privacy Forum;
- U.S. National Institute of Standards and Technology;
- Hydro One – Toronto Hydro – Ontario Power Generation;
- Extensive media outreach including The Economist, CBC, Toronto Star and an Op-Ed in the Globe and Mail.

Conclusions

- Lead with ***Privacy by Design*** – embed privacy into the design specifications of information technologies, accountable business practices and operations;
- Take it a step further – change the paradigm from "zero-sum" to "positive-sum," where both privacy *and* security, as well as privacy *and* energy conservation, can be delivered, thereby raising *overall* levels of protection;
- When you change the paradigm, you then change the mindset: you can deliver *both* privacy AND security, not as a mutually exclusive "either/or" (essentially a false dichotomy) but as the doubly enabling "win-win;"
- The future of privacy may very well depend on embedding privacy into Design – let's make it a reality!

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