Privacy by Design: Smart Privacy for the Smart Grid

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

Klaus Kursawe
European Network for Cyber Security and Radboud University
The Hague, The Netherlands

IEEE International Conference on Smart Grid Engineering
Ontario Institute of Technology
August 29, 2012

Presentation Outline

1. *Changing the Paradigm*
2. *Privacy by Design: The Gold Standard*
3. *Engaging Engineers*
4. *2012: Year of the Innovator*
5. *Implementing Privacy by Design: The Smart Meter Case*
6. *Positive-Sum Smart Grid*
7. *Conclusions*

The Decade of Privacy by Design

Setting the Stage:

Why We Need to Change the Paradigm

The Future of Privacy

Change the Paradigm to

Positive-Sum,

NOT

Zero-Sum

Positive-Sum Model

Change the paradigm
from a zero-sum to
a "positive-sum" model:
Create a win-win scenario,
not an either/or (vs.)
involving unnecessary trade-offs
and false dichotomies …

replace the "vs." with "and"

Privacy by Design:
The 7 Foundational Principles

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

Adoption of "Privacy by Design" as an International Standard

Landmark Resolution Passed to Preserve the Future of Privacy

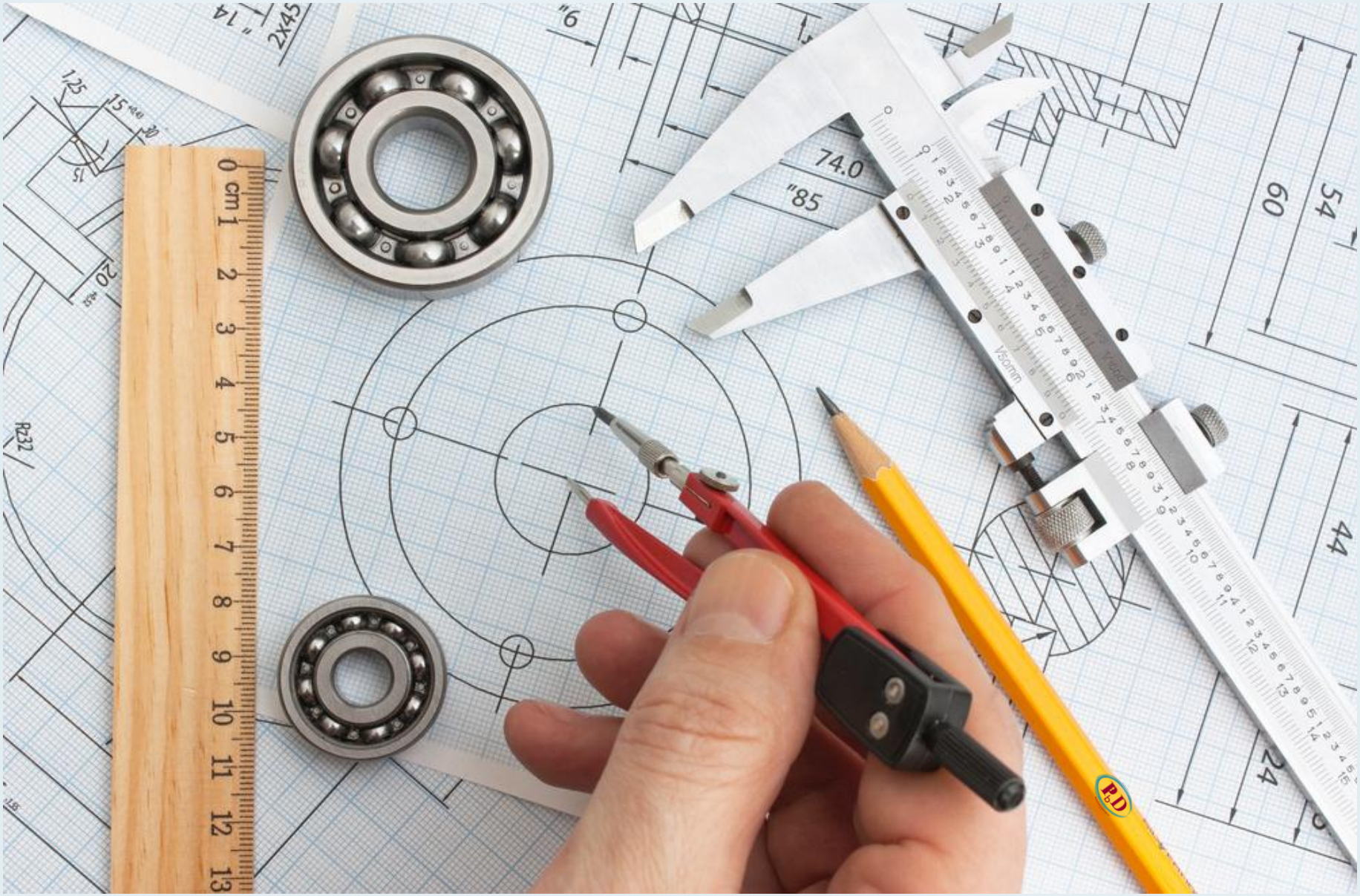
By Anna Ohlden – October 29th 2010 - http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy

JERUSALEM, October 29, 2010 – A landmark Resolution by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, was approved by international Data Protection and Privacy Commissioners in Jerusalem today at their annual conference.
The resolution recognizes Commissioner Cavoukian's concept of *Privacy by Design* - which ensures that privacy is embedded into new technologies and business practices, right from the outset - as an essential component of fundamental privacy protection.

Full Article:

http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy

2011: Year of the Engineer



Engaging Technical Teams

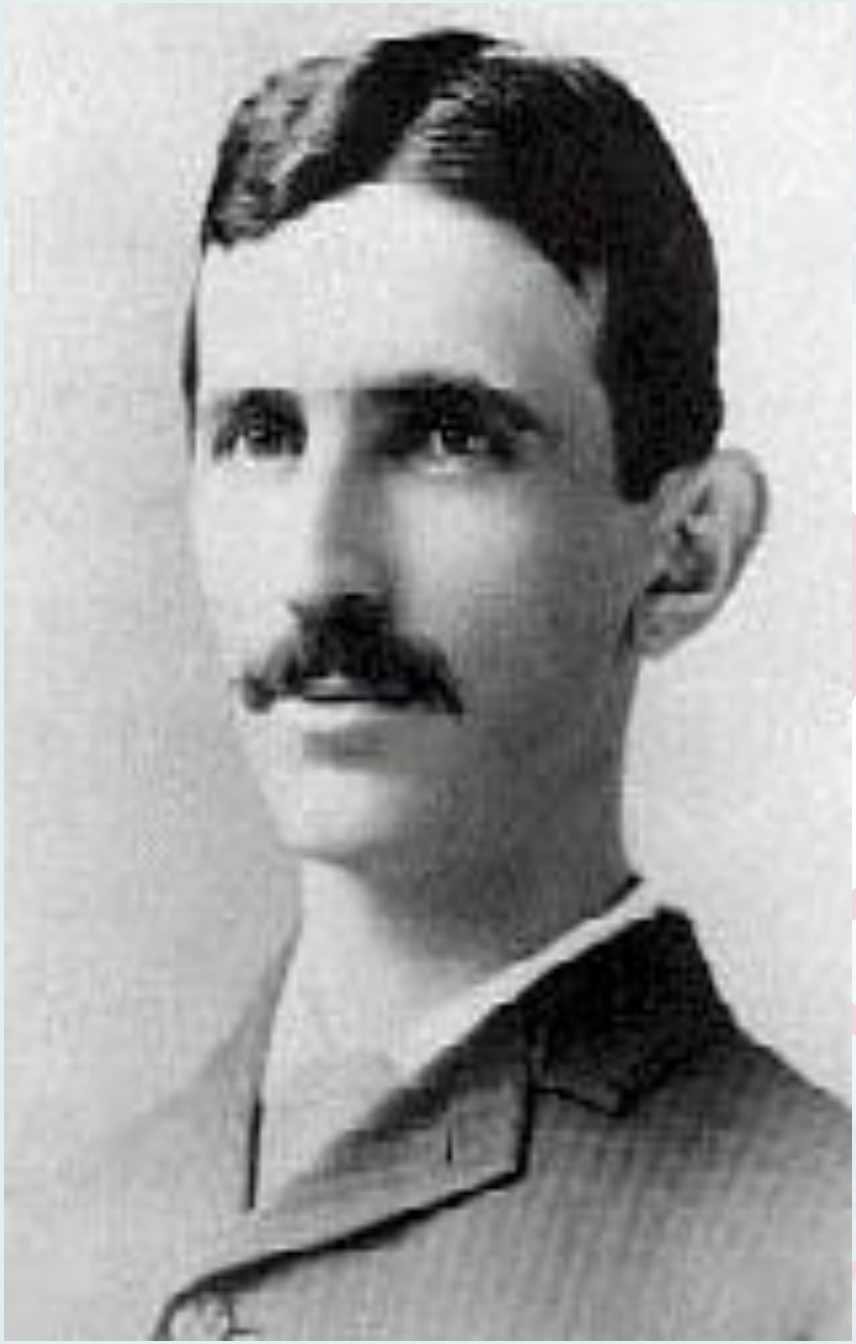
Privacy by Design and the Internet Engineering Task Force (IETF)

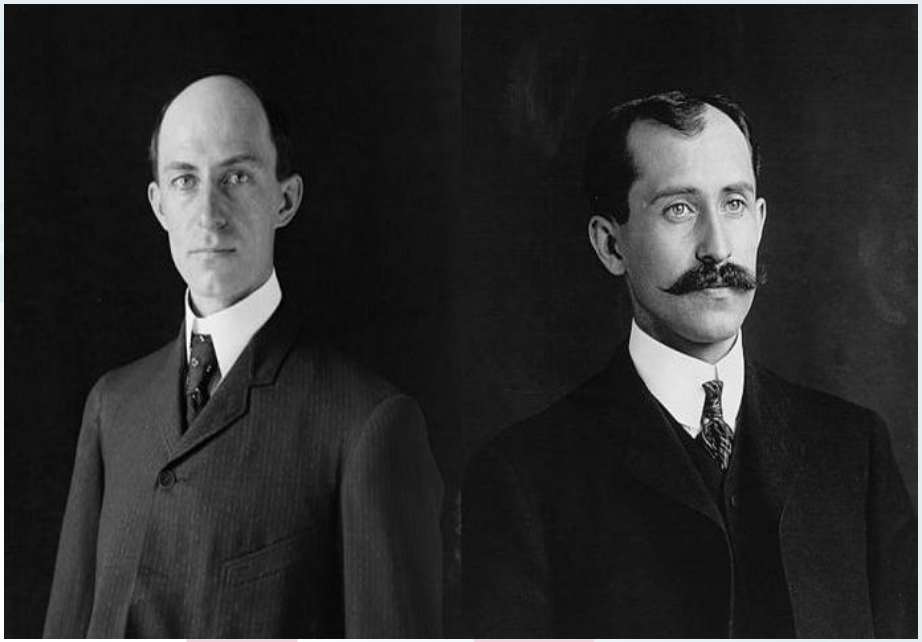
*"The concept of **Privacy by Design** has gotten a lot of attention over the past few years and within the IETF we have tried to investigate how we can consider privacy in the design of protocols and architectures in a more systematic way … in protocols and architectural designs."*

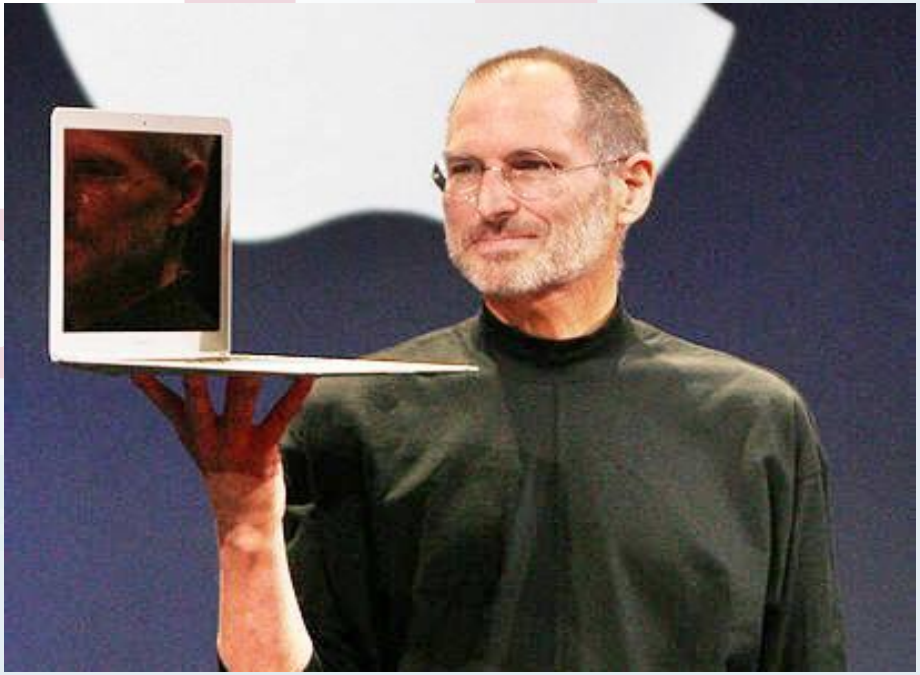
"We have started to shed more light on privacy in the IETF by organizing a privacy workshop to solicit input from the technically minded privacy community, to create an IETF privacy directorate, and to start the work on a number of documents to offer more guidance to engineers."

— *Privacy Considerations for Internet Protocols*, Internet Engineering Task Force (IETF), www.ietf.org

2012:
Year of the Innovator







Why *Privacy by Design* and the Smart Grid?

"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

"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**

ON ONO

WEDNESDAY, MAY 12, 2010 ✦ TORONTO STAR ✦ A23

CANADA

Can smart grid know too much?

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

TANYA TALAGA
QUEEN'S PARK BUREAU

The time you jump into the shower in the morning, the time you finally flick off that TV at night – even the time you set your home security alarm.

Ontario's privacy czar wants to keep the information secret.

Personal privacy must remain paramount as the "smart grid" electricity system is built around the province, said Ann Cavoukian, Ontario's information and privacy commissioner.

As the grid collects information on power usage and smart meters are installed in Ontario homes to track consumption data, that personal information could represent a treasure trove for hackers, thieves or marketers, said Cavoukian, in her annual report released Tuesday.

"Imagine the enormous interest in this information – not only by marketers and companies but unauthorized third parties like the bad guys, thieves who'll know when you are not at home," Cavoukian said in an interview.

Now is the time to continue to install privacy safeguards around the grid as it grows, she said.

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

Energy Minister Brad Duguid said he is taking Cavoukian's advice "very seriously" and is putting measures in place by controlling who has access to the information.

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

Yet before the switch was flicked on the program, all bases should have been examined and covered, said Progressive Conservative energy critic MPP John Yakabuski.

"We've talked about them having a serious rethink about smart meters from the get-go and every day we find more reasons why they should be doing that," Yakabuski said.

The infrastructure supporting the smart grid system will be soon be capable of letting consumers know their hourly and real-time energy use, Cavoukian said. "They can develop patterns of behaviour when you are away from the home," she said. "This thing has to be protected like Fort Knox."

In the not-so-distant future, "smart" appliances will be able to send in even more gritty details on how we live our lives to companies that provide electrical power. The sharing of that data should concern consumers, Cavoukian said.

"Think about every single appliance in your house reporting, in real time, your energy use. What will develop over time is a library of personal information relating to a profile of your personal energy use. When you watch TV, what time of day, when you eat, when you sleep and wake," she said.

Ontario must stay proactive on this, she said. "Right now is the ideal time to ensure no one gets this information other than the people who get it now – Toronto Hydro and Hydro One."

The privacy commissioner is working with both on how electrical companies should set standards. The companies will not give out any personal data without the consent of the consumer, she said.

"This is a treasure trove of information. We want to make sure privacy is the default."

THEY KNOW WHEN YOU ARE SLEEPING ...

SHUTTERSTOCK IMAGE

THEY KNOW WHEN YOU'RE AWAKE ...

RICHARD LAUTENS/TORONTO STAR FILE PHOTO

THEY KNOW WHEN YOU'RE IN THE SHOWER

SHUTTERSTOCK IMAGE

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

Implementing Privacy by Design: The Smart Meter Case

- **Data aggregation** techniques for meter data that do not reveal individual meter readings;
- Solutions may be implemented on existing smart meters with only a minimal increase in computational overhead;
- Modern crypto can provide a powerful building-block towards the implementation of *Privacy by Design*.

IEEE International Conference on Smart Grid Engineering (SGE'12)

Implementing *Privacy by Design*: The Smart Meter Case

Ann Cavoukian
Information and Privacy Commissioner
Toronto, Ontario, Canada
Commissioner@ipc.on.ca

Klaus Kursawe
Institute for Computing and Information Science
Raboud University Nijmegen
Nijmegen, The Netherlands
kursawe@cs.ru.nl

***Abstract*— The principles of *Privacy by Design* are gaining increasing support by policymakers and regulators and have been put forth as guidelines for smart meter deployments both in Europe and North America. For concrete implementations, however, it can be daunting as to what an electricity network operator should do to design privacy principles into their system. In the following paper, we outline the case of smart meter implementations, and propose aggregation protocols and cryptographic technologies that can be used to concretely implement *Privacy by Design* at the level of meter data, leading to not only privacy protection but at the same time, achieving a positive business impact.**

Keywords- smart meter, privacy, security, customer information, smart meter data, Privacy by Design

I. INTRODUCTION

With an aging infrastructure, modernization efforts are underway to make the current electrical grid "smarter." The infrastructure that will support the Smart Grid is envisioned to: provide consumers with more choices on when and how much they use; self-heal in case of disruptions such as natural disasters; be resilient against physical and cyber attacks; provide better energy quality and more efficient delivery and; link to alternative energy sources. The installation of advanced networks and communications technology will allow for data to be collated into understandable and actionable information for consumers and utilities.

One major component in this transformation to a Smart Grid is the smart meter, which will allow for real-time measurements of energy usage and interaction between the electricity provider (utility) and the consumer. Smart meter data is intended to allow for the development of an array of new services and efficiencies for both the consumer and the utility. Such end-user components and activities involving consumers, however, will tend to increase the collection, use and disclosure of personal information.

Privacy concerns arise when there is a possibility of discovering personal information such as the personal habits, behaviours and lifestyles of individuals inside dwellings, and to use this information without the consent of the consumer for purposes other than for the provision of electricity, such as marketing. Thus, the Smart Grid and smart metering will necessitate the emergence of a new relationship between utilities and individuals, centered on customer engagement and trust. Privacy and data security will be the dual cornerstones of this new relationship, with *Privacy by Design (PbD)* as its base to establish and maintain consumer trust and confidence.

In this paper, we outline why privacy needs to be considered at the earliest stage of advanced metering systems development. In addition, we also bring to light recent research that demonstrates data aggregation techniques for meter data, thereby not revealing individual meter readings. These techniques provide utilities with the granular meter data needed for load management, billing, and fraud or other security functions. This approach is a good example of *PbD* because it allows for the protection of customer privacy while maintaining, the quality of and potentially increasing, the data available to utilities for Smart Grid operations. Importantly, these prototypes have also shown that the solutions can be implemented on existing smart meters, with only a minimal increase in computational overhead. This demonstrates that modern cryptography is widely applicable even in constraint environments, and can provide a powerful building-block towards the implementation of the *PbD* principles.

II. PRIVACY AND THE ONGOING GROWTH OF THE SMART GRID

One of the greatest engineering achievements of the 20th century, electrical grids are the largest machines on earth. However, 100 years after their infrastructure was first built, they require updating to provide for new 21st century goals to make the grid efficient, reduce the impact on the environment, link up to alternative energy sources and provide for more consumer involvement and choice.

The ongoing growth of the Smart Grid is changing the role of the utility. Historically, energy providers focused on maintaining consistent supply at the lowest possible cost; interactions with customers largely involved billing and minimizing credit risk. With the Smart Grid, the promise for consumers is the increased ability to understand how they use energy, and help manage energy consumption better. To this end, an array of new services and various tools are being developed and deployed to allow consumers to see their energy use account information online, and in comparison with their neighbours. Also, smart devices in the home will further engage consumers in participating in energy reduction programs and savings plans offered by utilities.

The vast majority of the Smart Grid has to do with the operation of the power network (which consists of all systems, processes and devices used for the management of this network), to ensure the safe and reliable delivery of energy rather than pertaining to individual energy

Privacy by Design and Data Minimization

- Although de-identification is a tried and proven approach in settings where further research is to be conducted on the de-identified data, it is preferable to follow the principles of data minimization – collect as little personal data as possible;
- The first approach is data minimization in which data *aggregation* ensures that individual smart meter data cannot be disclosed in the first place;
- Aggregated data collected over a sufficiently large data set makes it generally impossible to determine individual data elements;
- The primary challenge for aggregated data is to ensure that the aggregation groups are chosen properly, to protect individual households and provide stable data for the intended use cases.

Aggregation Protocols for Smart Meter Data Minimization

- Billing Protocol using a Homomorphic Commitment Scheme;
- Diffie-Hellman based Private Aggregation Protocol (DiPA);
- Low Overhead Private Aggregation (LOPA).

Positive-Sum Smart Grid

- The positive-sum characteristic of these types of aggregation is that both Smart Grid operators benefit as well as energy consumers;
- When using privacy-preserving smart meter protocols, the granularity or frequency of meter readings raises little if any privacy concerns since this data is not transmitted from the smart meter, except with the consent of the consumer;
- As such, the frequency of meter readings can be increased without compromising consumer privacy.

Conclusions

- Lead with *Privacy by Design* – maintaining consumer confidence and trust will be essential;
- Enable both the Smart Grid *and* Privacy to grow in tandem – not one at the expense of the other – prevent the data breach … enable the service;
- Get smart about privacy by making it a priority – embed privacy into your technical specifications, architecture, systems, devices and business practices.
- If you don't lead with *Privacy by Design*, you may end up with privacy by chance – or worse, Privacy by Disaster!

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

Klaus Kursawe
European Network for Cyber Security and Radboud University
klaus.kursawe@encs.eu

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