Privacy by Design Breeds Creativity – Invites Innovation

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

Ontario Research and Innovation Optical Network
THINK Conference
April 25, 2013

Presentation Outline

1. *Privacy = Control*
2. *Positive-Sum, NOT Zero-Sum*
3. *Privacy by Design: The Gold Standard*
4. *The Age of Big Data and Privacy*
5. *Data Minimization and De-Identification*
6. *Privacy Drives Innovation – SmartData*
7. *Concluding Thoughts*

Privacy = Control

The Future of Privacy

Change the Paradigm to Positive-Sum, NOT Zero-Sum

It's Not A Zero-Sum Game

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 "vs." with "and"

The Decade of Privacy by Design

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

Privacy by Design:
Proactive in 30 Languages!

1. *English*
2. *French*
3. *German*
4. *Spanish*
5. *Italian*
6. *Czech*
7. *Dutch*
8. *Estonian*
9. *Hebrew*
10. *Hindi*
11. *Chinese*
12. *Japanese*
13. *Arabic*
14. *Armenian*
15. *Ukrainian*
16. *Korean*
17. *Russian*
18. *Romanian*
19. *Portuguese*
20. *Maltese*
21. *Greek*
22. *Macedonian*
23. *Bulgarian*
24. *Croatian*
25. *Polish*
26. *Turkish*
27. *Malaysian*
28. *Indonesian*
29. *Danish*
30. *Hungarian*

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

"Big Data"

- Each day we create **2.5 quintillion** bytes of data – **90%** of the data today has been created in the past 2 years;
- **Big Data** analysis and data analytics promises new opportunities to gain valuable insights and benefits, (e.g., improved load management, better assets management, new programs and services etc.);
- However, it can also enable expanded surveillance, on a scale previously unimaginable;
- This situation cries out for a ***positive-sum*** solution**,** a ***win-win*** strategy: what is needed for ***Big Data*** is ***Big Privacy!***

Did You Know?
In the EU, individuals' consent will "almost always" be required for Big Data

"Organisations will almost always require individuals' free, specific, informed and unambiguous ***opt-in*** *consent in order to make use of personal data they have previously collected in 'Big Data' projects …"*

— EU Article 29 Working Party,
April 9, 2013
http://www.out-law.com

Big Data – Yes

Open Data – Yes

Personal Data – No!

Big Privacy – Radical Control

- User control is critical
- Freedom of choice
- Informational determination

Context is Key!

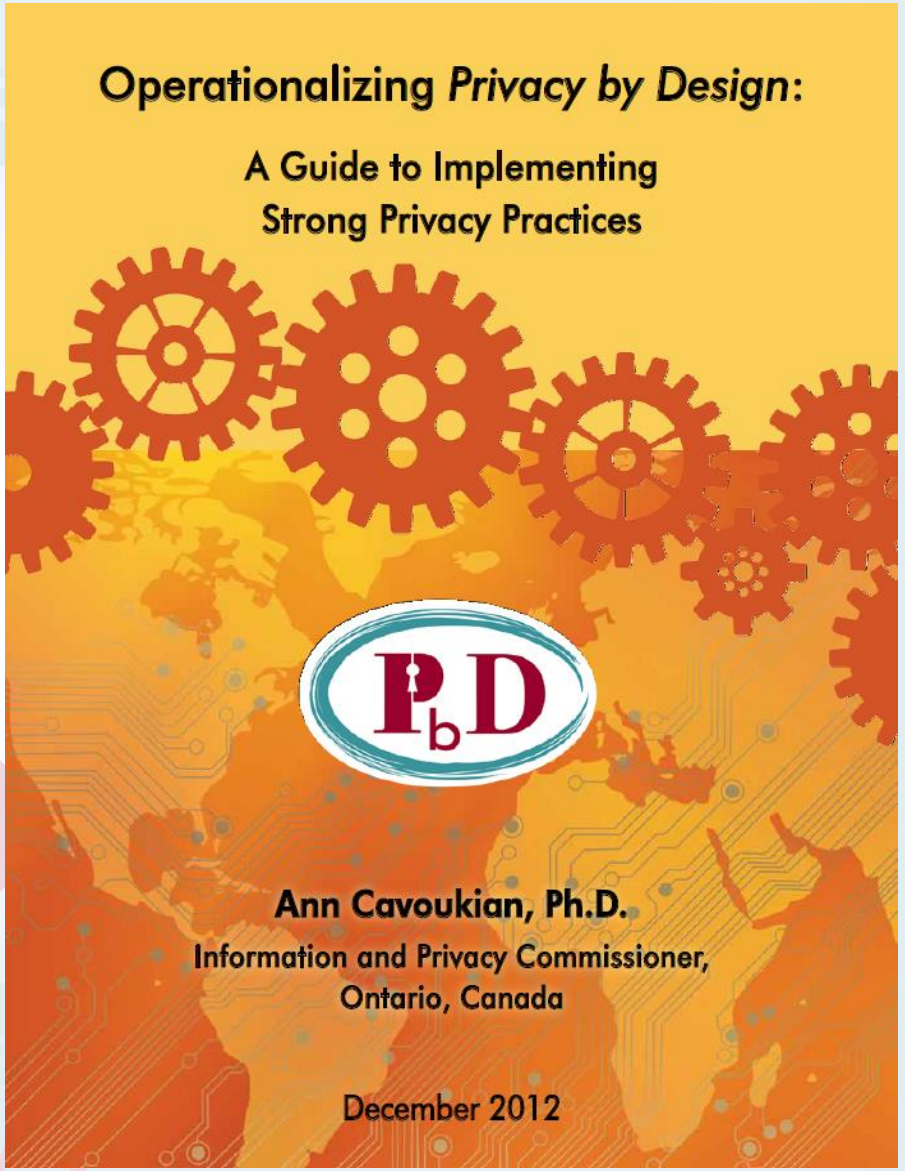
"Privacy by Design in the Age of Big Data"

- *The Big Difference with Big Data;*
- *"Sensemaking" Systems;*
- *Privacy by Design in the Age of Big Data;*
- *The Creation of a Big Data Sensemaking System through PbD.*

Operationalizing *Privacy by Design*

9 PbD Application Areas

- CCTV/Surveillance cameras in mass transit systems;
- Biometrics used in casinos and gaming facilities;
- Smart Meters and the Smart Grid;
- Mobile Communications;
- Near Field Communications;
- RFIDs and sensor technologies;
- Redesigning IP Geolocation;
- Remote Home Health Care;
- Big Data and Data Analytics.



www.privacybydesign.ca

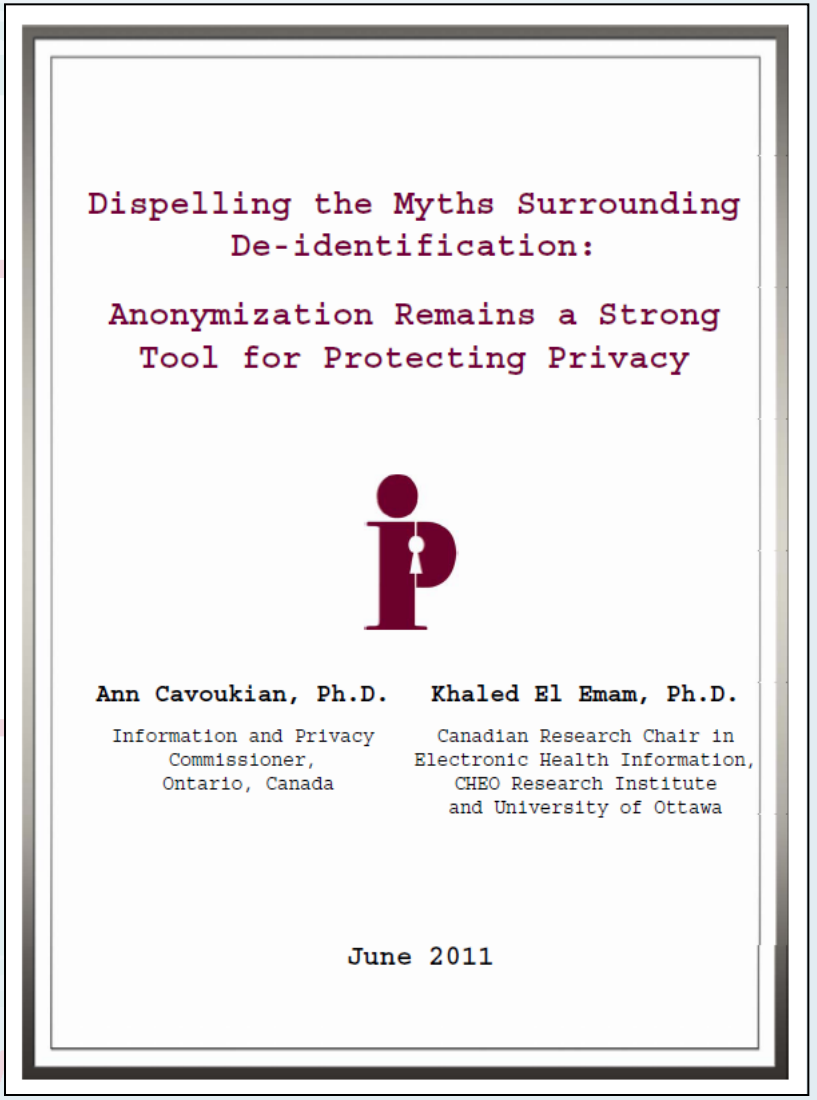
Data Minimization and De-Identification

Data Minimization

- Data minimization is the most important safeguard in protecting personally identifiable information, including for a variety of research purposes and data analysis;
- The use of strong de-identification techniques, data aggregation and encryption techniques, are absolutely critical.

Dispelling the Myths about De-Identification…

- The claim that de-identification has no value in protecting privacy due to the ease of re-identification, is a **myth**;
- If proper de-identification techniques and re-identification risk management procedures are used, re-identification becomes a very difficult task;
- While there may be a residual risk of re-identification, in the vast majority of cases, de-identification will strongly protect the privacy of individuals when additional safeguards are in place.


Dispelling the Myths Surrounding De-identification:

Anonymization Remains a Strong Tool for Protecting Privacy

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

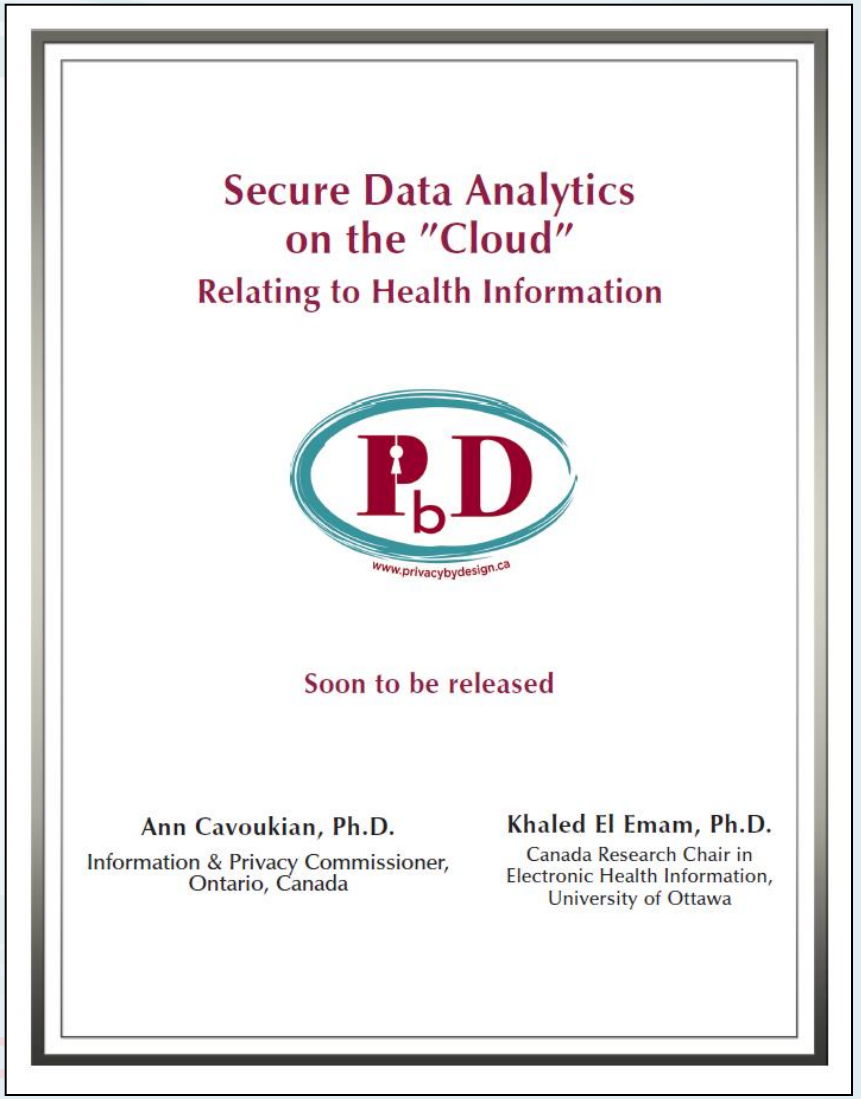
Khaled El Emam, Ph.D.
Canadian Research Chair in Electronic Health Information, CHEO Research Institute and University of Ottawa

June 2011

www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1084

Coming Soon –
Secure Data Analytics on the Cloud

- The Value of de-identification;
- Challenges in re-identifying de-identified information;
- De-identification in the context of privacy legislation;
- Re-identification risk assessment.



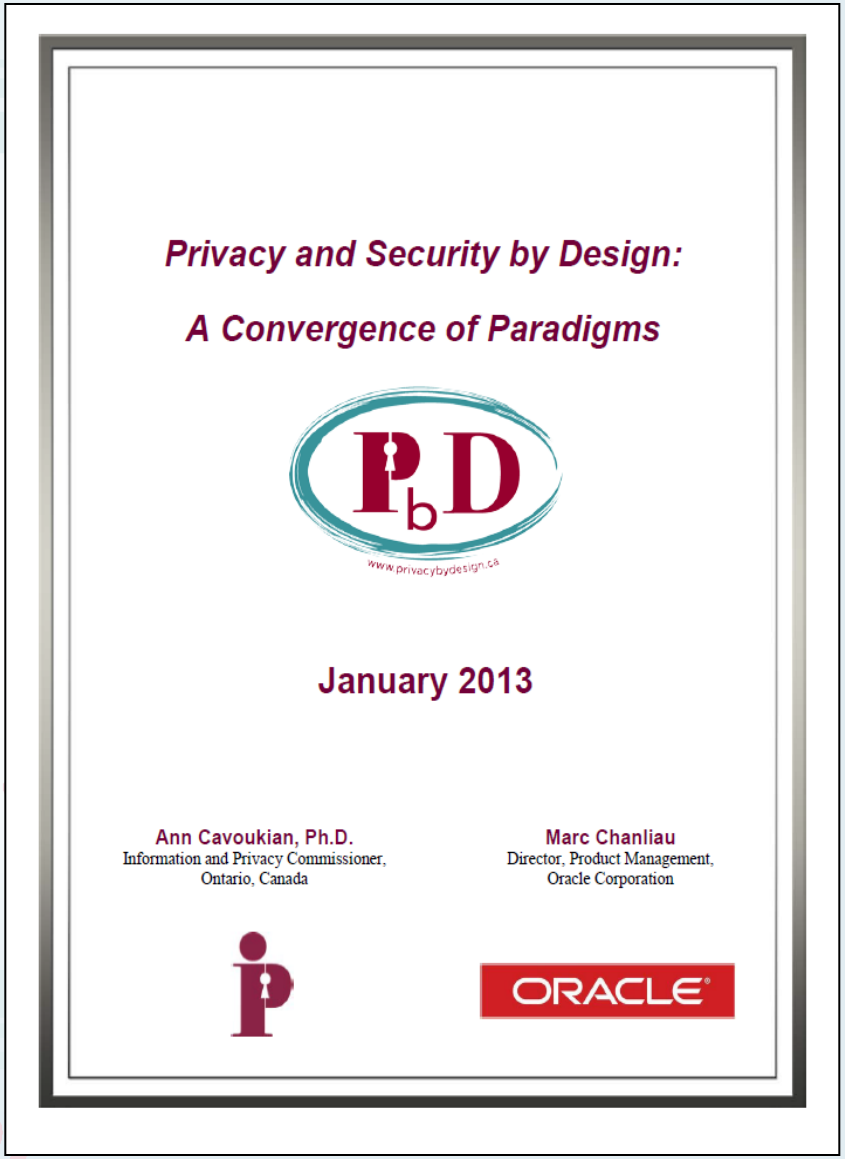
www.privacybydesign.ca

Homomorphic Encryption

- A form of encryption that allows computations to be carried out on encrypted data to obtain an encrypted result;
- Homomorphic describes the transformation of one dataset into another while preserving relationships between data elements in both sets;
- Homomorphic encryption allows you to make computations or engage in data analytics on encrypted values – data you cannot "read" because it is not in plain text, therefore inaccessible;
- May also be used to link two or more databases without the disclosure of any unique identifiers – positive-sum – win/win.

Enterprise Privacy and Security by Design

- The value to businesses of protecting privacy within an enterprise environment;
- The role of software engineers is at play in this context;
- Fostering a culture of respect for privacy within the enterprise;
- Good privacy = Good business;
- Gain a sustainable competitive advantage by embedding *Privacy by Design*.



www.privacybydesign.ca

Privacy Drives Innovation

Privacy Does *NOT* Stifle Innovation – It Breeds It!

- The argument that privacy stifles innovation reflects a dated, zero-sum mindset;
- The notion that privacy must be sacrificed for innovation is a false dichotomy, consisting of unnecessary trade-offs;
- The opposite is true – privacy drives innovation – it forces innovators to think creatively to find solutions that serve multiple functionalities;
- We need to abandon zero-sum thinking and adopt a positive-sum paradigm where both innovation ***and*** privacy may be achieved – we need a new playbook.

OASIS Technical Committee – *Privacy by Design for Software Engineers*

- Commissioner Cavoukian and Professor Jutla are serving as Co-Chairs of a new technical committee (TC) of OASIS (Advancing Open Standards for the Information Society) – *PbD-SE* (software engineers) TC;
- The purpose of *PbD-SE* is to provide *PbD* governance and documentation for software engineers;
- The *PbD* standards developed will pave the way for software engineers to code for *Privacy, by Design.*

"It Can't Be Done"

"The bolder the initiative, the harsher the criticism."

– Dr. Raymond Damadian, 1977

Invented of Magnetic Resonance Imaging (MRI)

The Next Evolution in Data Protection:

"SmartData"

- *SmartData* represents the future of privacy and greater control of personal information online;
- Intelligent "smart agents" will be developed and embedded into IT systems virtually – thereby creating "*SmartData*" – allowing one's data to protect itself;
- At the University of Toronto, this new "bottom-up" approach to Artificial Intelligence will revolutionize the field of AI.

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

SmartData:
It's All About User Control

It's All About Context:

- Evolving virtual cognitive agents that can act as your proxy to protect your personally identifiable data;

Intelligent agents will be evolved to:

- Protect and secure your personal information;
- Disclose your information only when your personal criteria for release have been met;
- Put the ***user*** firmly in control –
  Big Privacy, Radical Control!

www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1244

Concluding Thoughts

- It is much easier and more cost-effective to build in privacy up-front, rather than having to later bolt it on, after-the-fact; Privacy risks are best managed by proactively embedding *Privacy by Design*;
- *Privacy by Design* is not a theoretical construct – it is very real, and working on the ground, right now – it has been applied in multiple areas – you can have privacy *and* security, privacy *and* Big Data, data analytics … the sky's the limit;
- So, get smart – lead with *Privacy – by Design*, not 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

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