The Future is Now:
Embed Privacy – by Design, or Suffer the Consequences

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario, Canada

Southern Ontario Smart Computing Innovation Platform
MaRS Discovery District, Toronto
April 15, 2014

PbD
www.privacybydesign.ca

Presentation Outline

1. *Privacy by Design: The Gold Standard*
2. *Positive-Sum: The Power of "And"*
3. *Operationalizing Privacy by Design*
4. *Privacy = Control*
5. *Privacy Drives Innovation*
6. *SmartData: PbD 2.0*
7. *Concluding Thoughts*

The Decade of *Privacy by Design*

PbD
www.privacybydesign.ca

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

PbD
www.privacybydesign.ca

Privacy by Design:

Proactive in 36 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*
31. *Norwegian*
32. *Serbian*
33. *Lithuanian*
34. *Farsi*
35. *Finnish*
36. *Albanian*

PbD

www.privacybydesign.ca

Privacy by Design's Greatest Strength – Positive-Sum: *The Power of "And"*

Change the paradigm from
the dated zero-sum (win/win)
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"

PbD
www.privacybydesign.ca

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)*:

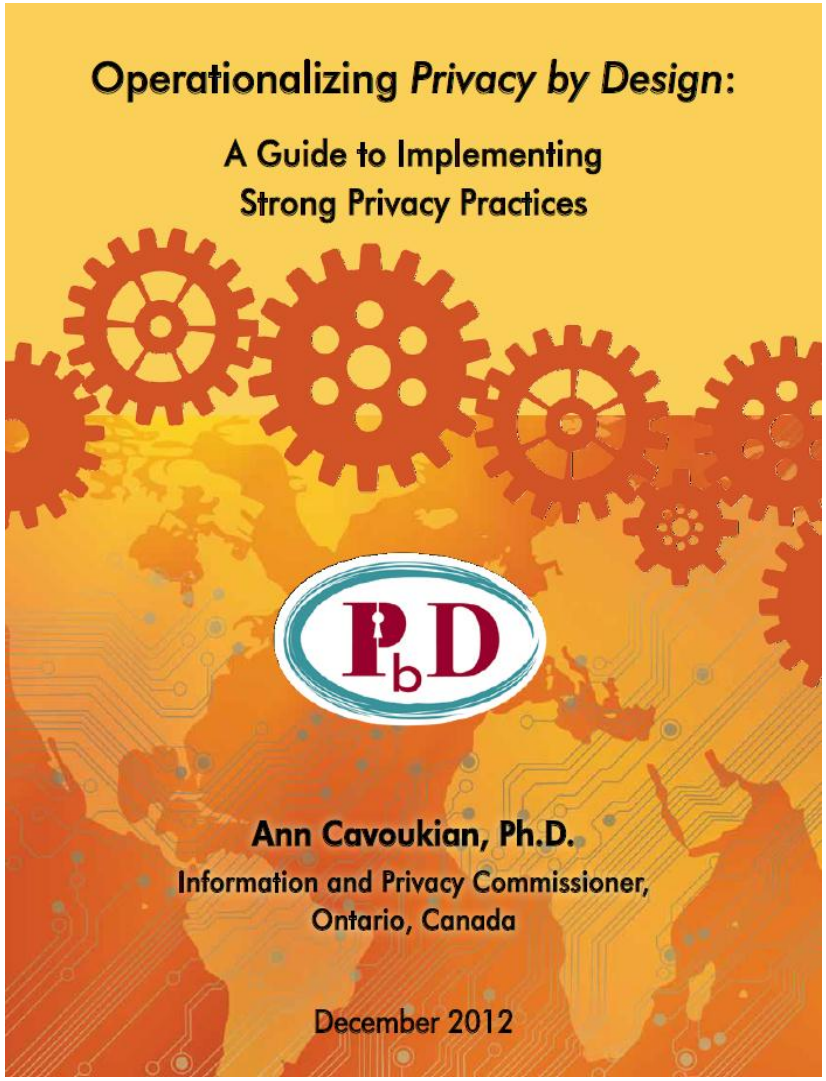
PbD

www.privacybydesign.ca

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.



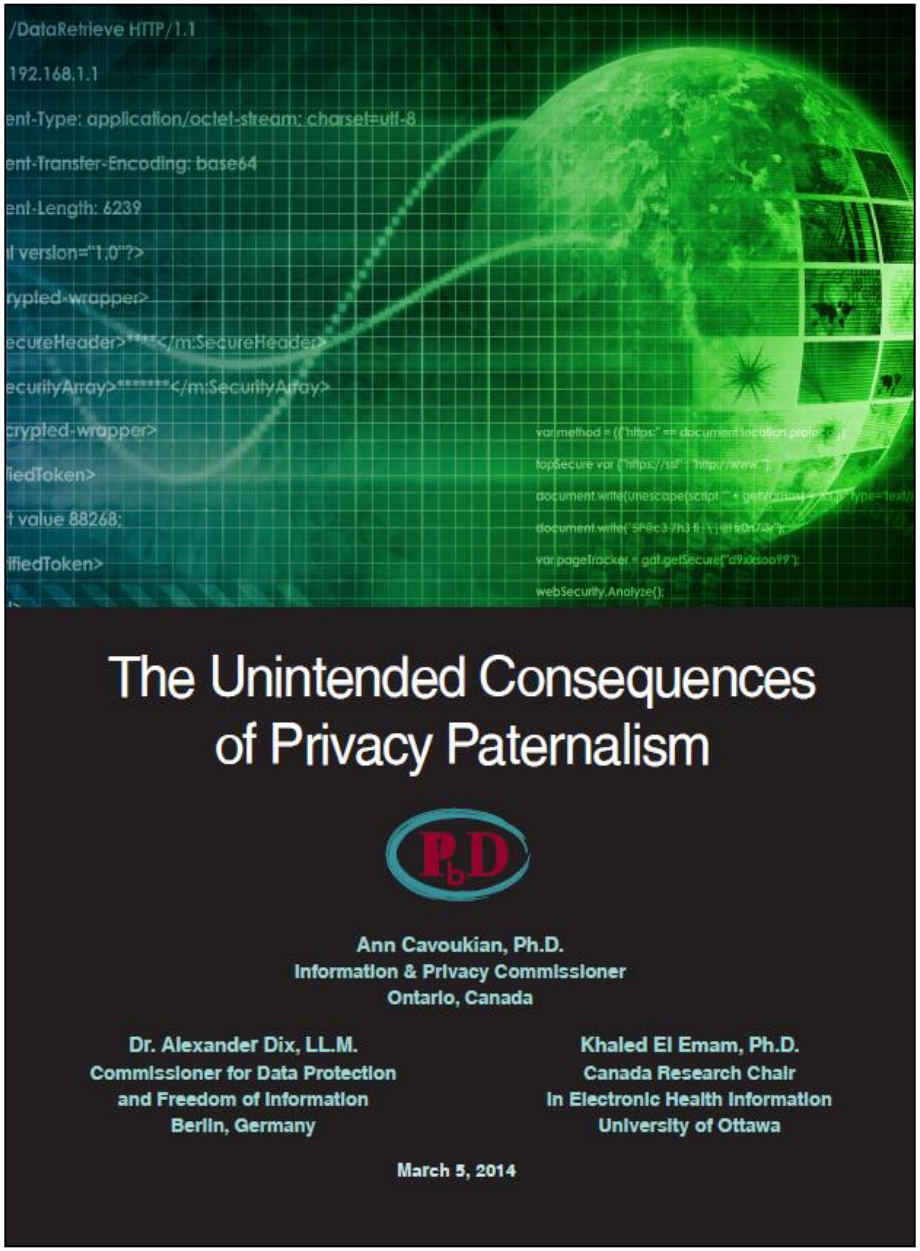
PbD
www.privacybydesign.ca

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

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

Privacy = Control

Personal Control
Freedom of Choice
Informational Self-Determination



www.privacybydesign.ca

Beware of the Backlash!

Harris Poll Shows NSA Revelations Dramatically Impacted Public's Behaviour

- **26%** of respondents said they are now doing far less banking online;
- Another **26%** of respondents said they are also doing less shopping online;
- **24%** said they are now less inclined to use email.

— welivesecurity.com
April, 2014

Financial Implications of NSA Revelations: U.S. Businesses to Lose Billions

*"There are discussions now that the NSA revelations will bring about losses to the U.S. IT industry of upwards of **$200 billion**. These are major impacts on an industry that is directly traceable to the concerns that non-U.S. citizens, governments, and industry have over whether they can trust U.S.-based companies."*

— Professor Ron Deibert,
September 13, 2013.

— Reza Akhlaghi,
A Candid Discussion with Ron Deibert,
Foreign Policy Association, September 13, 2013.

PbD
www.privacybydesign.ca

Target Targeted

- A breach of Target's networks resulted in the theft of 110 million credit and debit card records, with 70 million records containing addresses and telephone numbers;
- Experts have predicted that it may cost Target and Neiman Marcus up to **$550 million** to replace stolen account numbers –not taking into account any future penalties, credit monitoring expenses, lawsuits or security infrastructure upgrades;
- The theft of Target's customer data had a significant impact on the company's profit, falling more than **40%** in the fourth quarter; and down **46%** from last year.

Changing Attitudes

- **September 2013** – a Pew Research survey reported that **86%** of Americans had taken steps to remove or mask their digital footprints online;
- **68%** believed that existing laws are not strong enough to protect them.

— *A Second Front in the Privacy Wars*,
New York Times Editorial, February 23, 2014.

The Public Wants Privacy

*"More than **60%** of respondents to an Associated-Press poll said they valued their privacy more than anti-terror protections."*

— Eileen Sullivan,
AP-GfK poll: Americans value privacy over security,
January 27, 2014

Heartbleed

"Several news outlets reported that the U.S. NSA, which for years has worked hand-in-hand with researchers to find and fix these sort of bugs, knew about Heartbleed for two years, but said nothing."

— Michael Riley,
NSA Said to Exploit Heartbleed Bug for Intelligence for Years,
Bloomberg, April 12, 2014.

Canadians also Concerned About Online Privacy

- "Two-thirds (66%) of Canadians say they were concerned about the protection of their privacy."
- One-quarter say they were "extremely concerned."

— Commissioner Chantal Bernier,
Privacy Commissioner of Canada,
Metro News, April 8, 2014

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 will 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.

PbD
www.privacybydesign.ca

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 architectural designs in a more systematic way."*

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

PbD
www.privacybydesign.ca

Professor Lawrence Lessig on Technology and Privacy

"A technology should reveal no more information than is necessary … it should be built to be the least revealing system possible."

— Professor Lawrence Lessig,
Harvard Law School,
Author of "Code: Version 2.0"

PbD
www.privacybydesign.ca

SmartData:
Privacy by Design 2.0

Context is Key

The Next Evolution in Data Protection:

"SmartData"

Developed by Dr. George Tomko, at the Identity, Privacy and Security Institute, University of Toronto, *SmartData* represents privacy in the future, with greater control of personal information.

Intelligent "smart agents" to be introduced into IT systems virtually – thereby creating "*SmartData,*" – a new approach to Artificial Intelligence, bottom-up, that will contextualize the field of AI .

PbD
www.privacybydesign.ca

SmartData:
Embedding 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!

Next Steps:

Ryerson University's Privacy and Big Data Institute …

Where Big Data meets Big Privacy!

Win/Win, not Win/Lose

— Ryerson University Privacy and Big Data Institute

July 1,2014

Concluding Thoughts

- Privacy risks are best managed by proactively embedding the principles of *Privacy by Design* – prevent the harm from arising – don't wait for the breach;
- Focus on prevention: It is much easier and far more cost-effective to build in privacy, up front, rather than bolt it on after-the-fact;
- Abandon zero-sum thinking – embrace doubly-enabling, win/win systems: Big Data ***and*** Big Privacy;
- Get smart: lead with *Privacy – by Design*, not privacy by chance or, worse, *Privacy by Disaster!*

PbD
www.privacybydesign.ca

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

PbD

www.privacybydesign.ca