Data, Data Everywhere – The Need for Big Privacy in Big Data

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario, Canada

Privacy by Design User Forum

December 5, 2013

www.privacybydesign.ca

Presentation Outline

1. *Era of Expanded Surveillance*
2. *NSA/CSEC Surveillance*
3. *Privacy by Design: The Gold Standard*
4. *The Age of Big Data*
5. *Operationalizing Privacy by Design*
6. *Privacy Breeds Innovation*
7. *Concluding Thoughts*

Entering into an Era of Expanded Surveillance

- NSA/PRISM/Metadata
- Drones/Unmanned Aerial Vehicles (UAVs)
- Automatic Licence Plate Scanners (ALPs)
- Vehicle Black Boxes/GPS
- Video Surveillance (CCTV)
- Biometric Tracking

PbD
www.privacybydesign.ca

NSA/CSEC Surveillance

Edward Snowden Revelations

- Edward Snowden's revelations have profound implications for privacy, human rights, freedom, Internet governance, Internet commerce, international relations, and national security;
- Governments have largely concealed the size, scope, and purpose of their security programs, and in the process, have undermined citizen trust in government;
- Transparency in lawmaking is essential to the health of any democracy, particularly with respect to intrusive state powers;
- Efforts to weaken encryption standards, as well as to co-opt communications service providers not only threaten an open and secure Internet, they also set a chill at the heart of the North American Internet economy.

NSA Surveillance

Collecting the Data

- **Telephony Metadata Program** – collection of bulk telephone records;
- **PRISM** – collection of metadata and content from Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple;
- **Upstream –** collection of metadata and content from telco-fiber cables and infrastructure as data flows past ("Cable Tapping");
- **Follow the Money –** collection of data from international payments, banking, and credit transactions.

Processing the Data

- **Xkeyscore** – system used to amalgamate, process, and search collected data;
- **Marina** – computer metadata database used to examine users' browser experiences and gather "contact information/content;
- **Graphing Social Connections** – large-scale graph analysis based on NSA's collection of domestic and international metadata;

NSA/CSEC Surveillance

Undermining Encryption

- **Breaking Codes –** deployed custom-built, superfast computers to break codes with brute force;
- **Weakening Standards –** secretly inserted a "back door" into international encryption standards;
- **Backdoors –**NSA's Sigint Enabling Project engages U.S. and foreign IT industries to covertly influence and/or overtly leverage commercial products' designs to make them exploitable.

Communications Security Establishment Canada (CSEC)

- It was revealed that Communications Security Establishment Canada (CSEC) played a substantial role in the NSA's efforts to crack encrypted data;
- CSEC was in charge of the encryption standards process for the International Organization for Standardization in 2006, at which time the NSA finessed CSEC into handing over control of the standards process in order to get its preferred encryption code – *with a back door* - made into a worldwide standard.

NSA Revelations: Financial Implications

*"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

Civil Liberties vs. Security

6 out of 10 Americans *report that protecting the privacy rights and freedoms of U.S. citizens is more important than making sure they are safe from being harmed by terrorists.*

— *The Associated Press-NORC Center for Public Affairs Research, September 2013*

http://www.apnorc.org/projects/Pages/Civil-Liberties-and-Security.aspx

PbD
www.privacybydesign.ca

NSA and Privacy Rights

- ***75%*** *of Americans polled say the NSA programs are infringing on privacy rights;*
- ***47%*** *of Americans view surveillance programs as making little difference in U.S. security.*

— Washington Post-ABC News Poll, July 2013

http://www.presstv.com/detail/2013/07/24/315375/americans-concerned-about-privacy-poll/

It's Time for a Change:

Change the Paradigm to Positive-Sum,

NOT

Zero-Sum

Positive-Sum Model: *The Power of "And"*

Change the paradigm
from 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"

PbD
www.privacybydesign.ca

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 33 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*

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

Privacy by Design Centre of Excellence

- Developed especially for the Ontario Public Service and broader public sector, such as municipalities, hospitals and universities.
- While I am proud that *PbD* has spread throughout the world, I would like to ensure that *PbD* retain its prevalence here in Ontario – which is why I teamed up with the Ontario Public Service to develop the "*Privacy by Design Centre of Excellence;*"
- The *PbD Centre of Excellence* will provide leadership and best practices to ensure that privacy is embedded as the default in both new and existing Ontario government programs;
- Please visit http://coe.privacybydesign.ca/ to find out how you can get involved and make a difference for the protection of privacy in Ontario.

PbD
www.privacybydesign.ca

BECOME A *PRIVACY BY DESIGN* AMBASSADOR

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

PbD

www.privacybydesign.ca

“Big” Data

"Big Data"

- Each day we create **2.5 quintillion** bytes of data
  – **90%** of all data was created in the past 2 years;
- **Big Data** analysis and data analytics promise new opportunities to gain valuable insights and benefits
  – new predictive modes of analysis;
- However, it will also enable expanded surveillance, increasing the risk of unauthorized use and disclosure, on a scale previously unimaginable.

The Age of Big Data … Open Data *and* Big Privacy

Big Data – Yes

Open Data – Yes

Personal Data - No

- *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.*

PbD
www.privacybydesign.ca

Personal Data Ecosystem

Personal Data Ecosystem (PDE)

- There is a growing need to break down information silos, liberate data, and allow individuals to decide how best to use and share their personal data;
- The PDE is a set of companies, organizations, and policymakers who believe that individuals should be in control of their own personal information – employing new tools, technologies, and policies to empower them;
- The rise of the PDE may be the biggest leap forward in the protection of privacy since the advent of the privacy policy (which is no longer read).

The Respect Network

- Consists of an alliance of over 30 companies, building the world's first peer-to-peer network of personal and business clouds;
- The Respect Trust Framework won the Privacy Award at the 2011 European Identity Conference;
- It is currently at the beta stage, and will open for personal and business members in mid-2014.

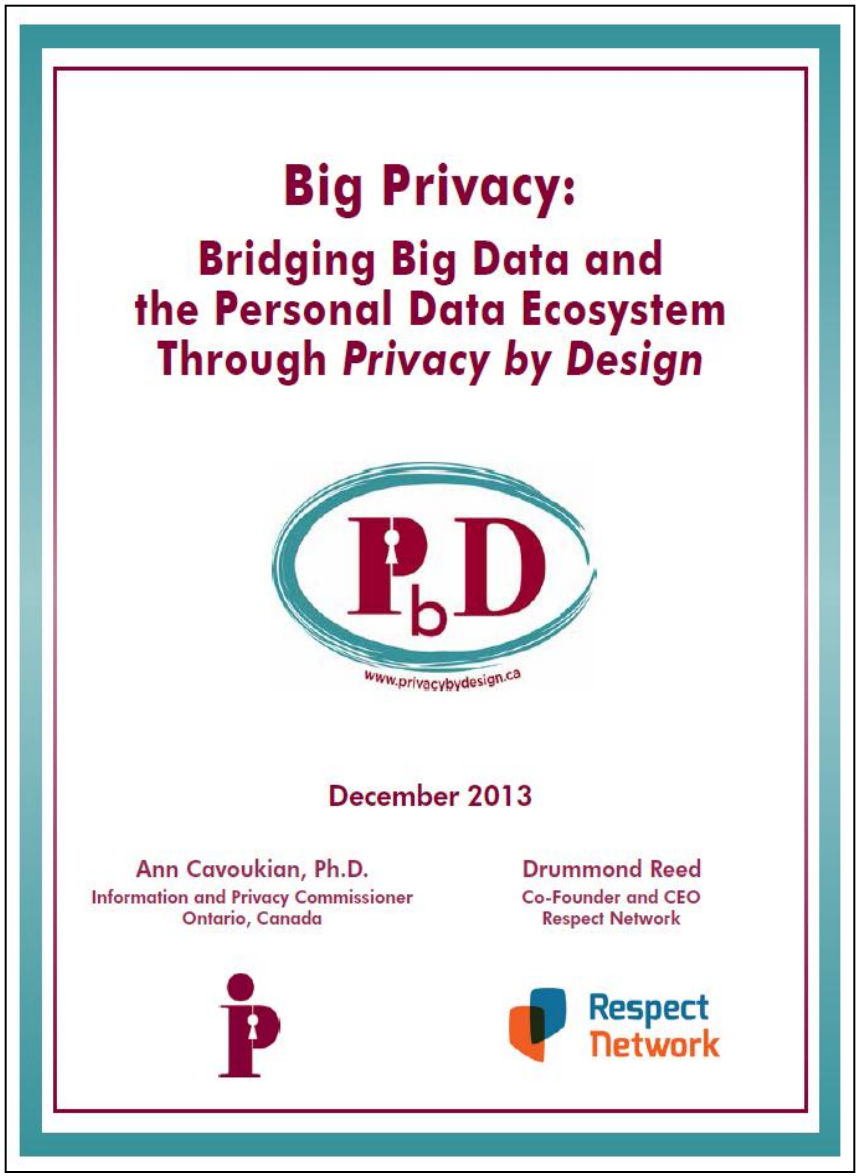
Launch of Our New White Paper with the Respect Network:

Big Data Meets Big Privacy!

December 5, 2013

PbD
www.privacybydesign.ca

" … Big Data derives economic value from its use of personal data – to such an extent that if personal information is considered to be the "new oil," then Big Data is the machinery that runs on it."



PbD
www.privacybydesign.ca

BIG Privacy – Radical Control

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

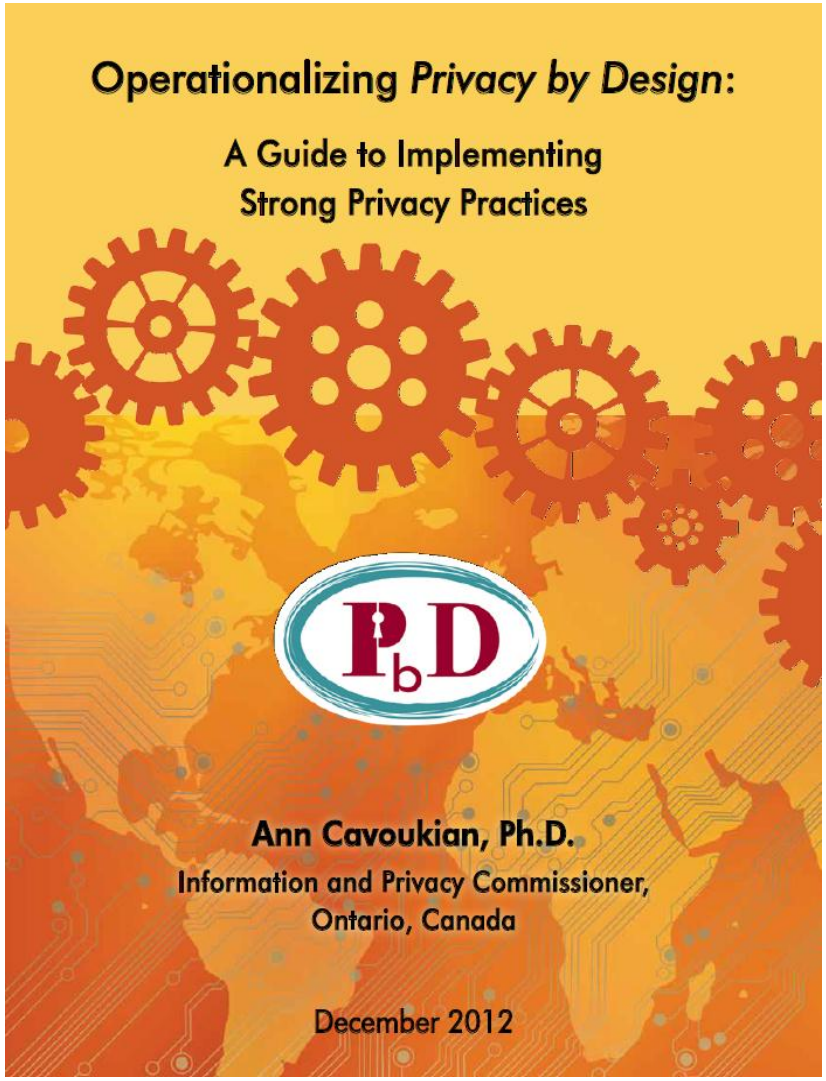
Context is key!

Operationalizing Privacy by Design

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

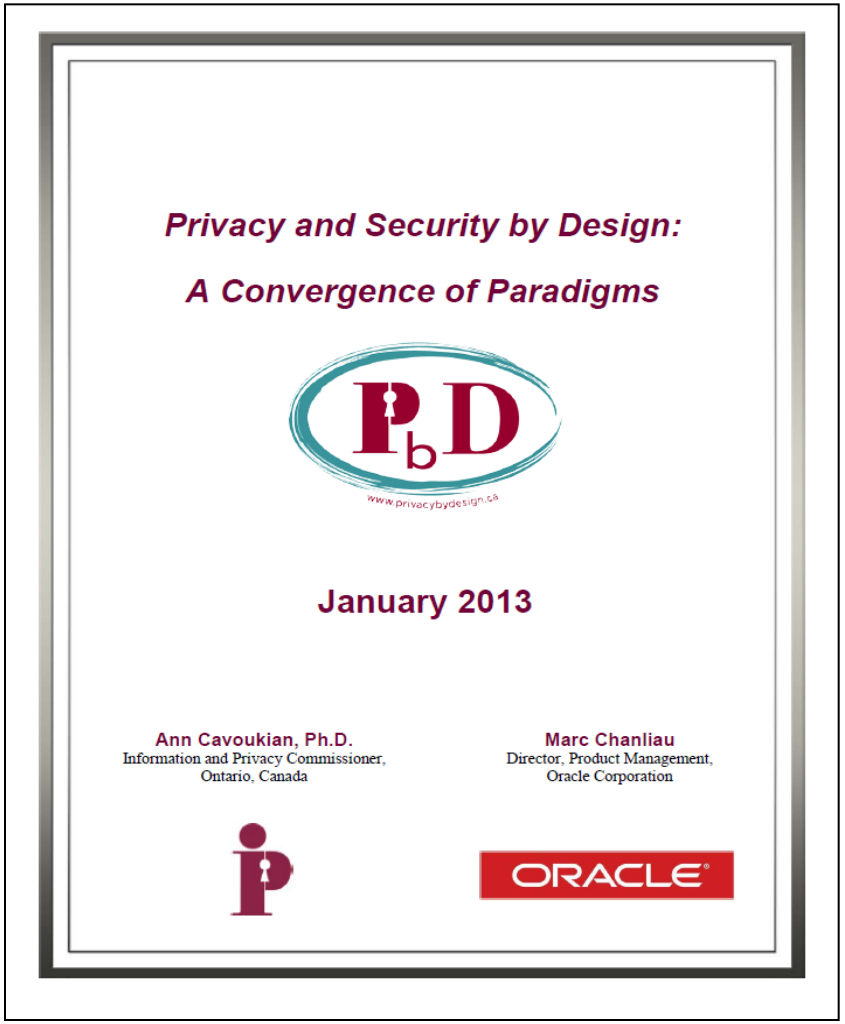
OASIS Technical Committee – *Privacy by Design for Software Engineers*

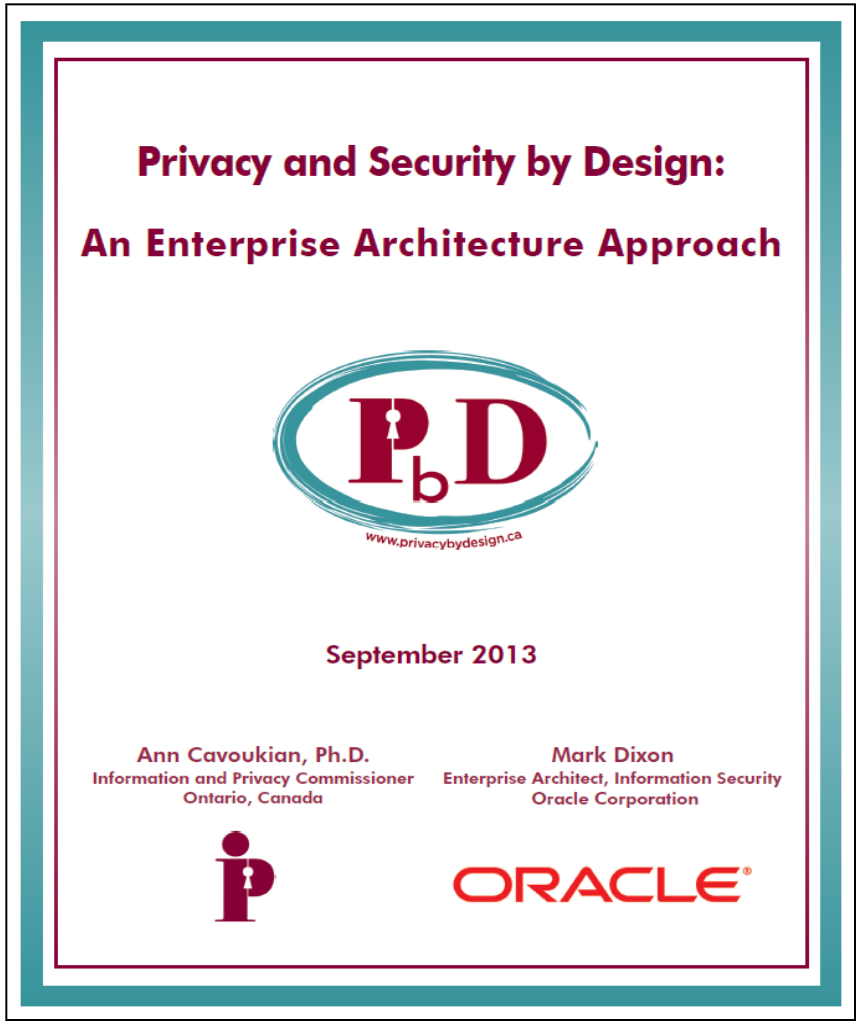
- Commissioner Cavoukian and Professor Jutla are the Co-Chairs of a new technical committee (TC) of OASIS (Advancing Open Standards for the Information Society) – "*PbD-SE* (software engineers) TC;"
- The purpose of *PbD-SE* is to provide *PbD* governance and documentation for software engineers;
- The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

Carnegie Mellon University – *Privacy By Design*

- New Master's degree program for privacy engineers is being offered by Carnegie Mellon University, School of Computer Science;
- The Master of Science in Information Technology-Privacy (MSIT-Privacy) is a 12-month program that began in the fall semester of 2013;
- The program will emphasize the concept of *Privacy by Design*, in which safeguards are incorporated into the design of systems and products from the very beginning of the development process;
- Students who complete the Master's program will be prepared for the International Association of Privacy Professionals (IAPP) Certified Information Privacy Professional certification exam.

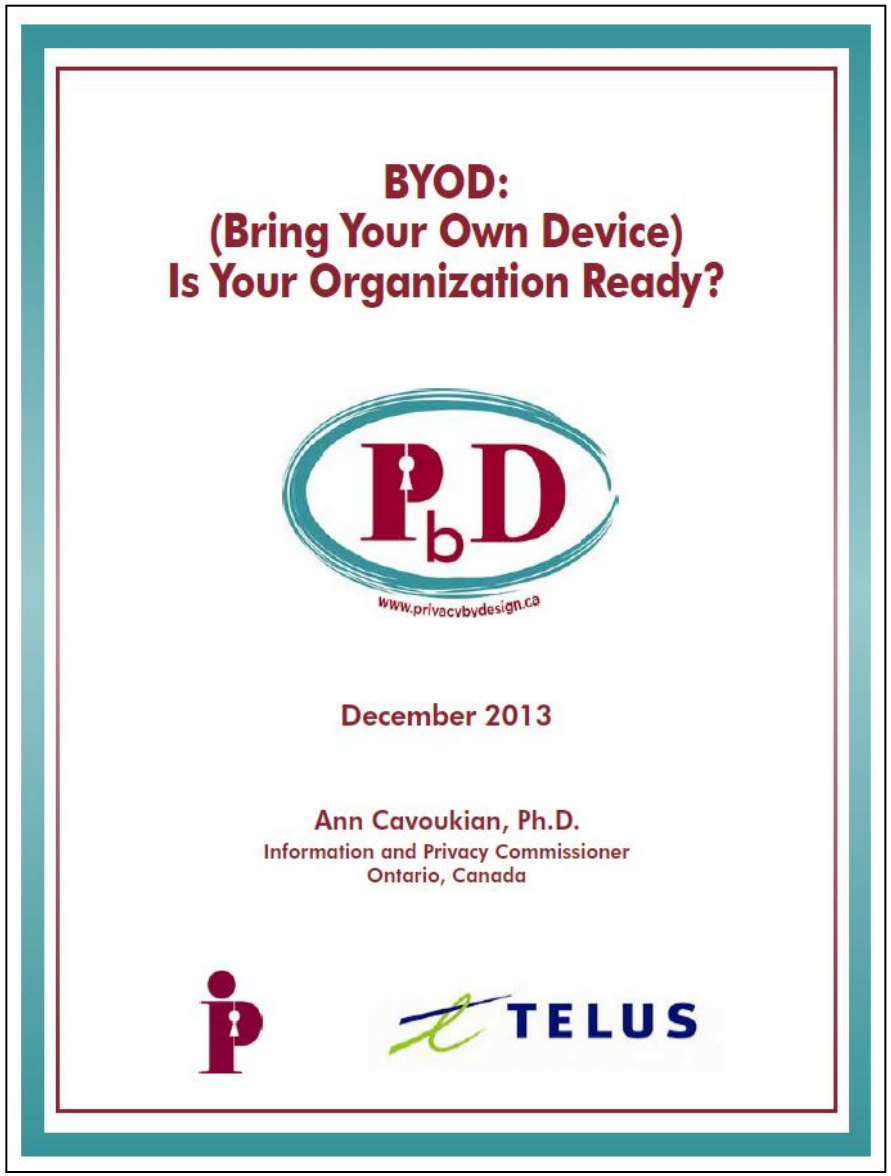
Enterprise Privacy and Security by Design





PbD
www.privacybydesign.ca

"Canadian companies outpace their global counterparts when it comes to adopting the bring-your-own-device in the workplace, while simultaneously leading the world in the greatest number of companies losing the most corporate data through employee-operated mobile devices."



PbD
www.privacybydesign.ca

The future of Privacy will rest on creativity, innovation and collaboration

Microsoft®

RIM®

ELOQUA

Adobe®

Google

AMERICAN EXPRESS

IBM

RYERSON UNIVERSITY

MaRS

bionym

SC WorldCongress ENTERPRISE DATA SECURITY 2009 CONFERENCE & EXPO

IPSI

ASU ARIZONA STATE UNIVERSITY

berlin

Technische Universität Berlin

web 2.0 SUMMIT

UNIVERSITY OF ALBERTA

PbD

www.privacybydesign.ca

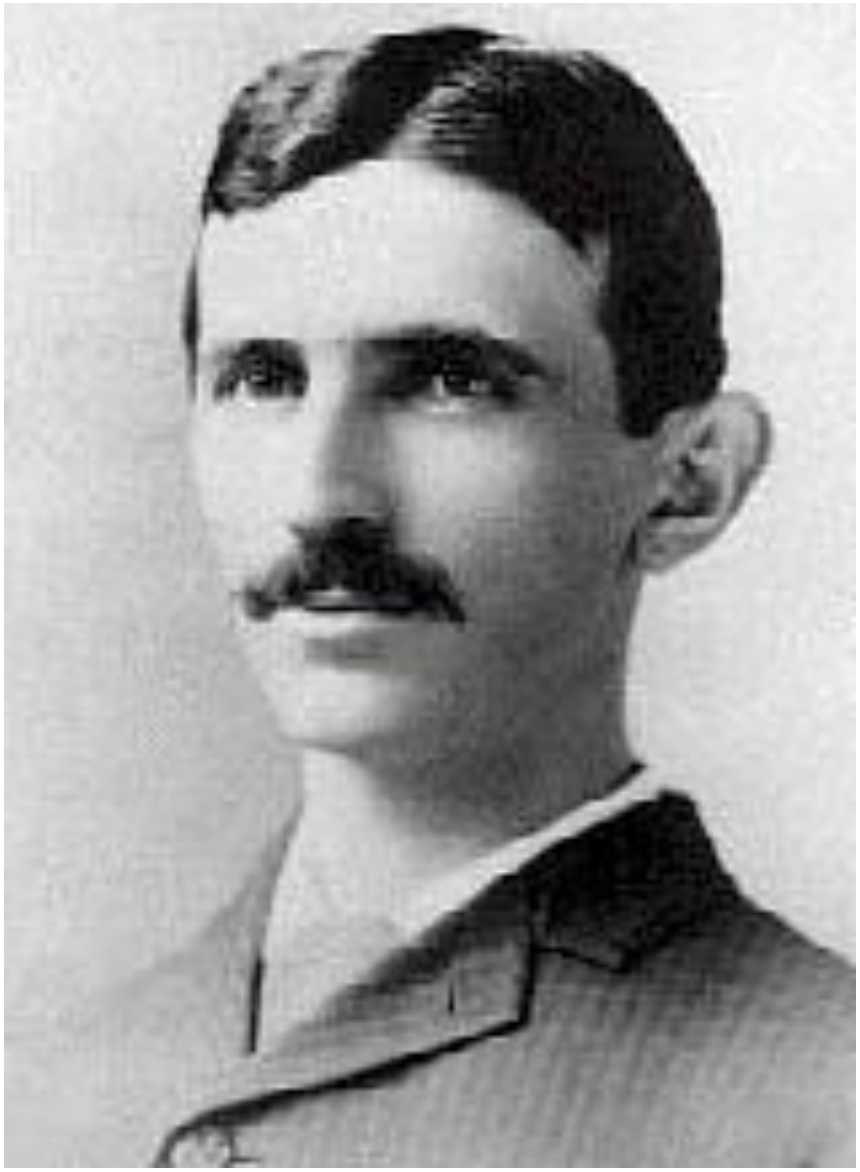
Privacy by Design and the Internet Engineering Task Force (IETF)

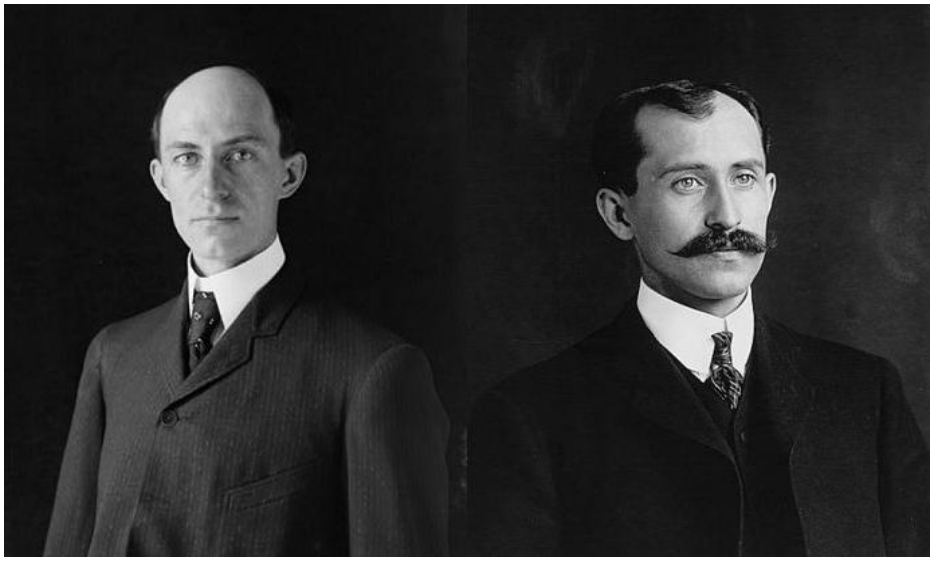
*"The concept of **Privacy by Design** has gotten a lot of attention over the past few years and within the IETF we have tried to investigate how we can consider privacy in the design of protocols and architectures in a more systematic way … in protocols and architectural designs."*

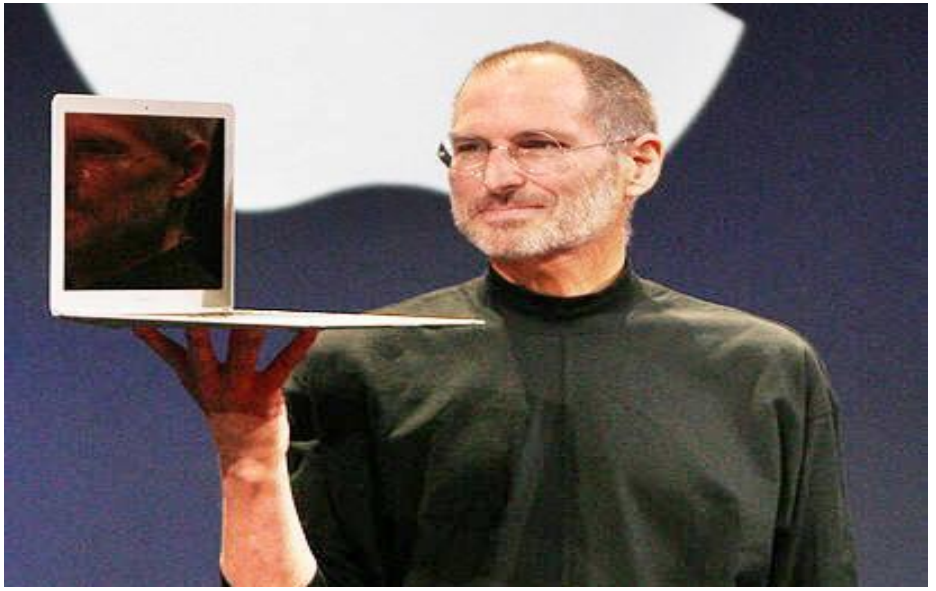
"We have started to shed more light on privacy in the IETF by organizing a privacy workshop to solicit input from the technically minded privacy community, to create an IETF privacy directorate, and to start the work on a number of documents to offer more guidance to engineers."

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

PbD
www.privacybydesign.ca







www.privacybydesign.ca

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

“It Can’t Be Done”

“The bolder the initiative, the harsher the criticism.”

– Dr. Raymond Damadian, 1977

Inventor of Magnetic Resonance Imaging (MRI)

Concluding Thoughts

- Lead proactively with *Privacy by Design;*
- Change the paradigm from the dated "zero-sum" to the doubly-enabling "positive-sum strategy;"
- Deliver *both* privacy AND security, privacy AND Big Data, in an empowering "win-win" paradigm – abandon false trade-offs;
- Embed privacy as a core functionality:
  the future of privacy (and freedom) may very well depend on it!

PbD
www.privacybydesign.ca

How to Contact Us

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner, 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