

*Privacy by Design –
Leading the Way to Preserving Our Freedom,
Minimizing Surveillance*

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

Mozilla

Mountain View, California

November 15, 2013

Presentation Outline

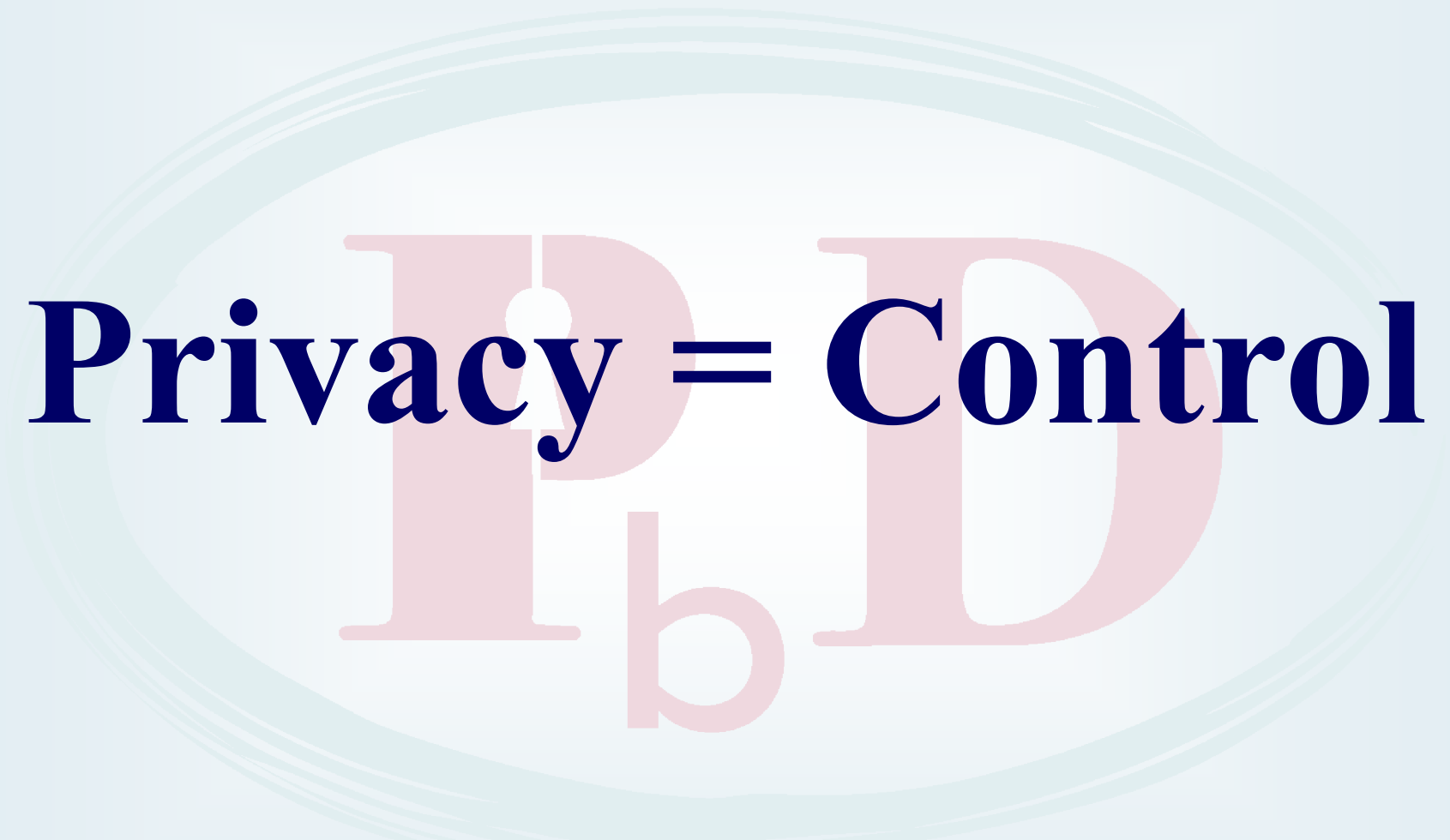
- 1. Privacy – Essential to Freedom*
- 2. Change the Paradigm to Positive-Sum*
- 3. Privacy by Design: The Gold Standard*
- 4. Do Not Track (EFF: “Stop Watching Us”)*
- 5. Engaging Engineers and Innovators*
- 6. Privacy-Protective Surveillance*
- 7. Conclusions*

Privacy is Essential to Freedom: A Necessary Condition for Societal Prosperity and Well-Being

- Innovation, creativity and the resultant prosperity of a society requires freedom;
- Privacy is the essence of freedom:
Without privacy, individual human rights, property rights and civil liberties, the conceptual engines of innovation and creativity, could not exist in a meaningful manner;
- Surveillance is the antithesis of privacy:
A negative consequence of surveillance is the usurpation of a person's limited cognitive bandwidth away from innovation and creativity.

Privacy \neq Secrecy

Privacy is *not* about having something to hide



Privacy = Control

www.privacybydesign.ca

BIG Privacy – Radical Control

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

Context is key!

The Future of Privacy

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

Positive-Sum Model: *The Power of “And”*

*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”

The Decade of Privacy by Design



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

Privacy by Design:

Proactive in 31 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

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**.



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.

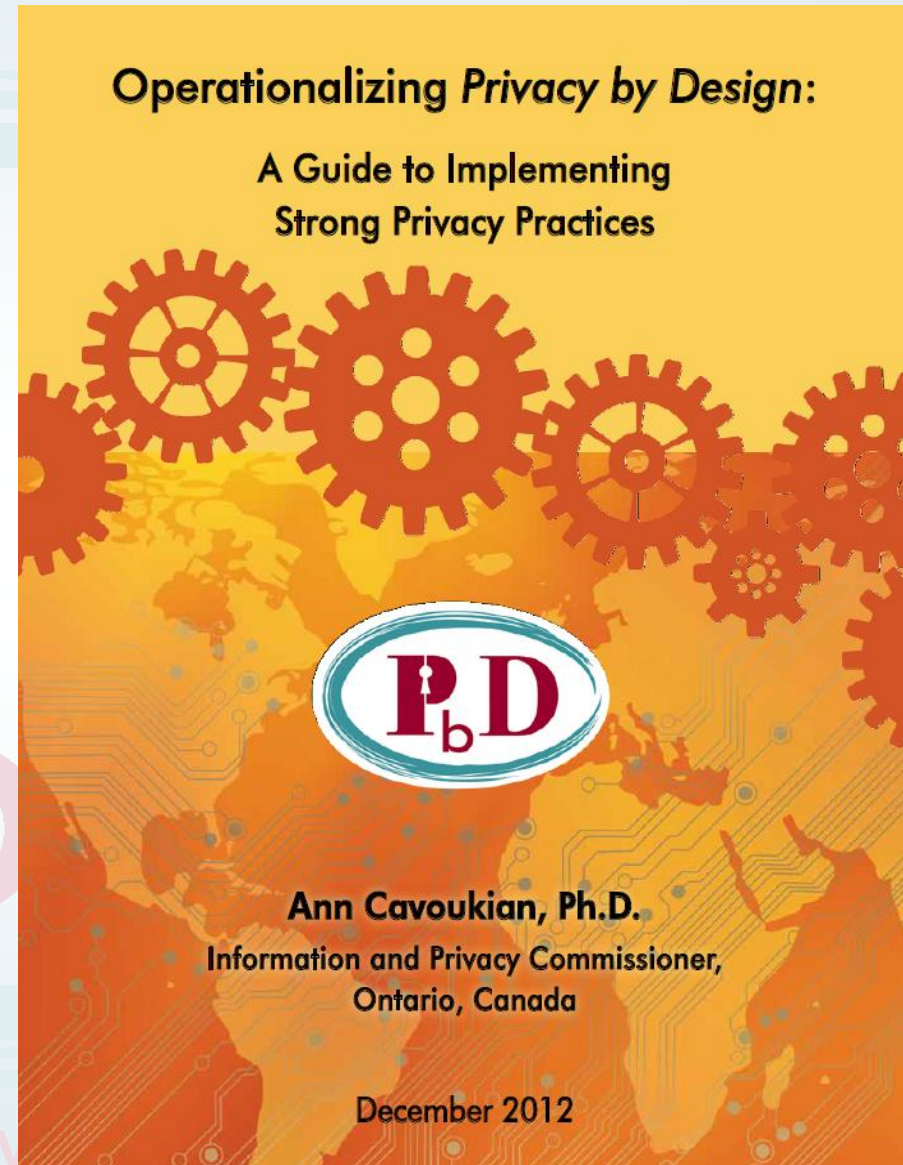
Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

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*):

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.



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*.

Carnegie Mellon University – *Privacy By Design*

- New Master's degree program for privacy engineers to be 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 begins 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.

Ryerson University:

Digital Media Zone

Digital Media Zone (DMZ) School of Engineers, is a unique setting where students and companies can turn their innovations into market-ready products – producing solutions to real-world, real-time problems – *such as building privacy into new technologies*

<http://digitalmediazone.ryerson.ca/>

Flybits – a research team based at DMZ that focuses on ubiquitous and pervasive computing, with the goal of using mobile devices to enhance interpersonal communications, *while conserving privacy.*

Mozilla's Lightbeam and Do Not Track: *Setting A Privacy Precedent*

“The clearest losers in Mozilla’s plan will be companies that track users without their knowledge.” [It’s all about transparency].

— Craig Timberg,
[Firefox Web browser to move ahead plan to block tracking](#),
The Washington Post, June 19, 2013.

Consumers Want Do Not Track – by Default

“Seventy-five percent of the consumers we surveyed in the U.S. and Europe said they wanted DNT on, by default.”

— Brad Smith
Microsoft Executive Vice-President
December, 2012.

<http://www.bloomberg.com/news/2012-12-13/microsoft-rankles-advertisers-with-web-user-privacy-plan.html>

Do Not Track *(Cont'd)*

*“Most consumers want Do Not Track to mean exactly that: **do not** collect information that allows companies to track them across the Internet. This may seem obvious, but even the definition articulated by the FTC may fall short of these consumer expectations.”*

— Chris Jay Hoofnagle,
Director, Information Privacy Programs,
Berkeley Center for Law & Technology,
October, 2012.

Electronic Frontier Foundation

Stop Watching Us



STOP WATCHING US

HOME

NEWS

FAQ

GET INVOLVED ▾

PETITION

RESOURCES

CONTACT

GETTING THERE

THANK YOU

On October 26th thousands of you gathered on the steps of the capitol and sent a clear message to Congress: Stop Watching Us.

Stay involved: Message "Privacy" to 877877 using mobile SMS and we'll get in touch when it's time for action again.



www.youtube.com/watch?v=aGmiw_rrNzk



***Engaging Engineers
and Innovators***

www.privacybydesign.ca

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

www.privacybydesign.ca



Microsoft[®]



Adobe

ELOQUA

Google



RYERSON UNIVERSITY

MaRS



Technische Universität Berlin

GIPSI

ASU ARIZONA STATE UNIVERSITY

SC
WorldCongress
ENTERPRISE DATA SECURITY 2009
CONFERENCE & EXPO

web 2.0
SUMMIT



UNIVERSITY OF ALBERTA

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.”*

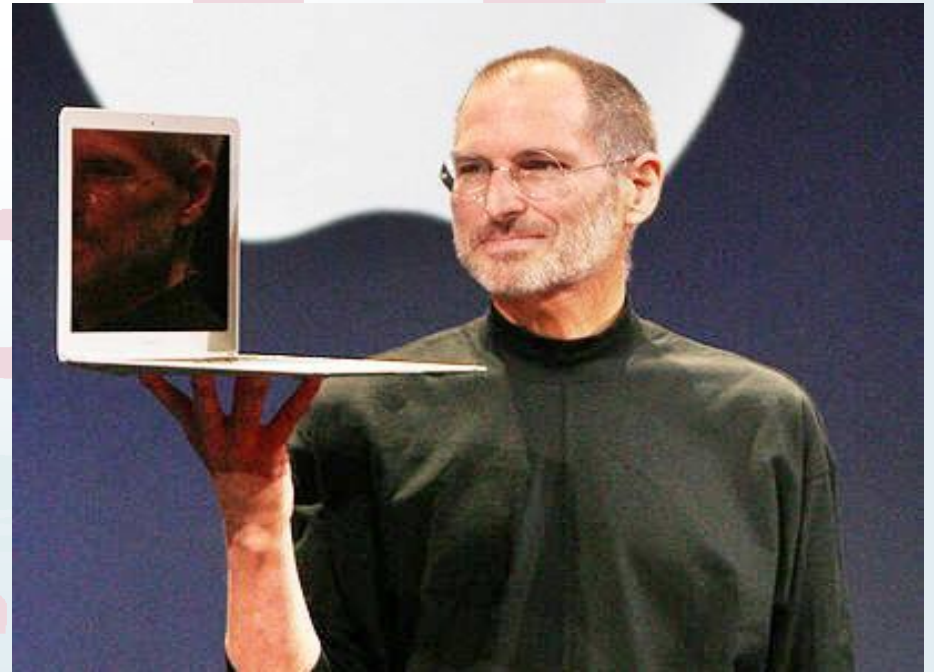
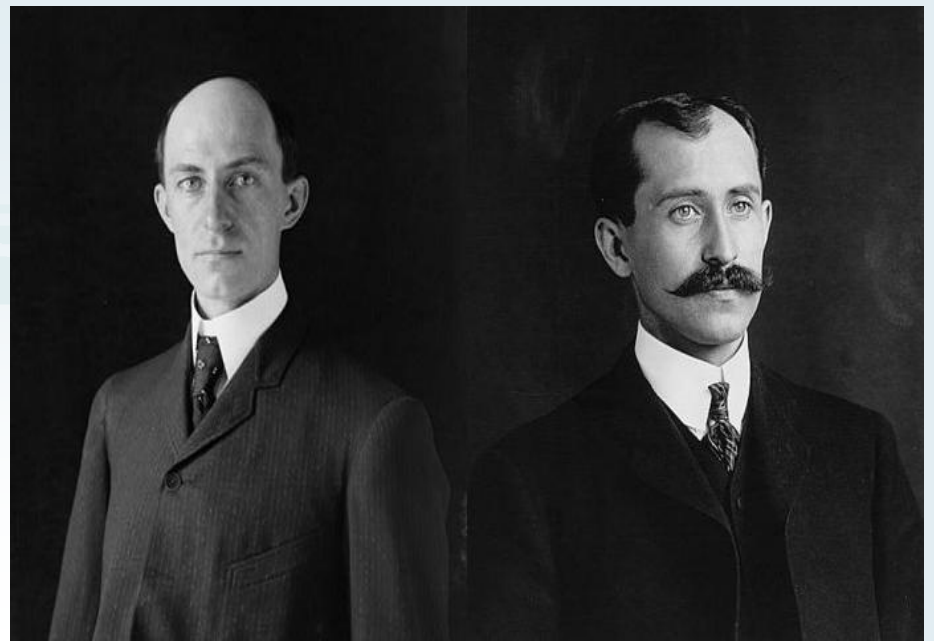
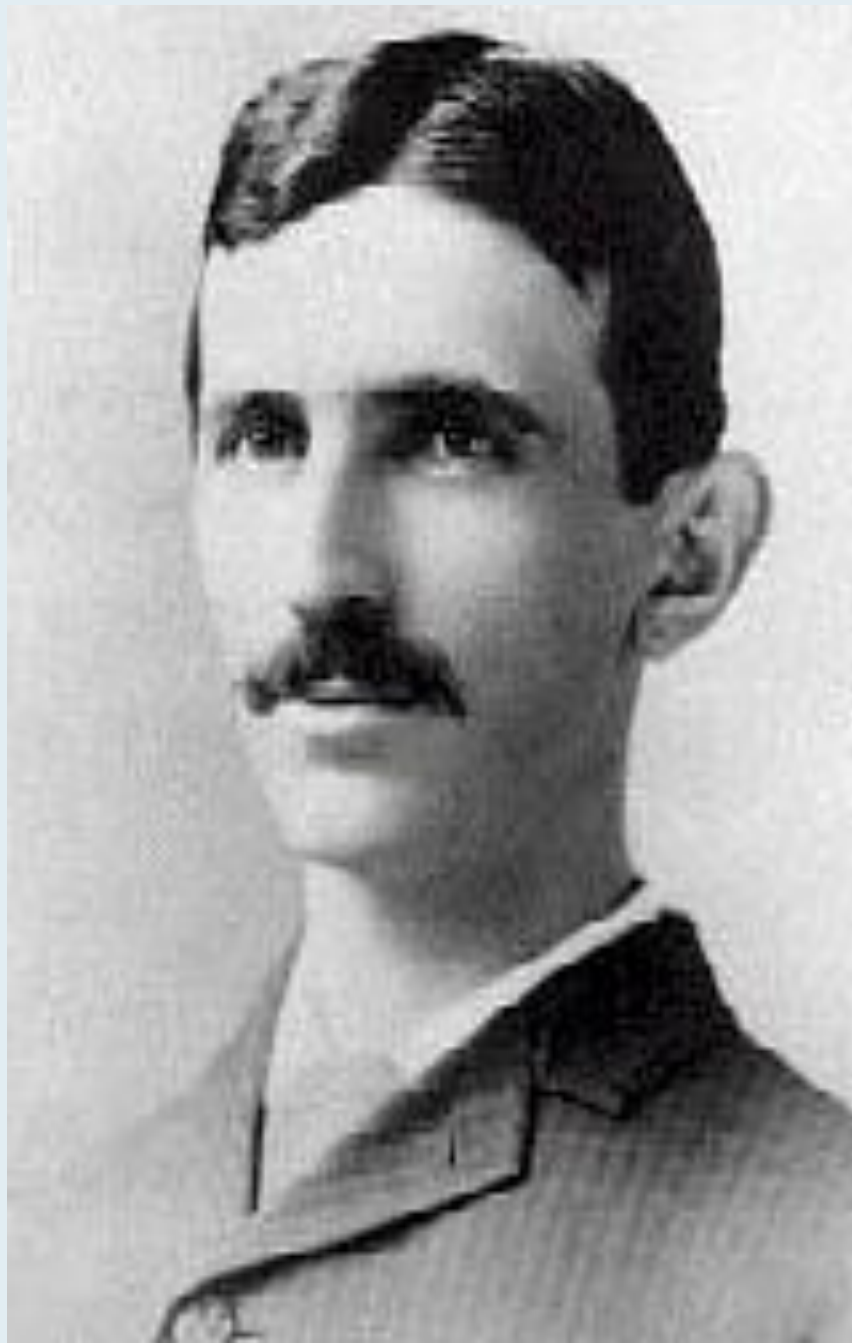
“We have started to shed more light on privacy in the IETF by organizing a privacy workshop to solicit input from the technically minded privacy community, to create an IETF privacy directorate, and to start the work on a number of documents to offer more guidance to engineers.”

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



***Privacy Drives
Innovation***

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.

“It Can’t Be Done”

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

– Dr. Raymond Damadian, 1977

Inventor of Magnetic Resonance Imaging (MRI)

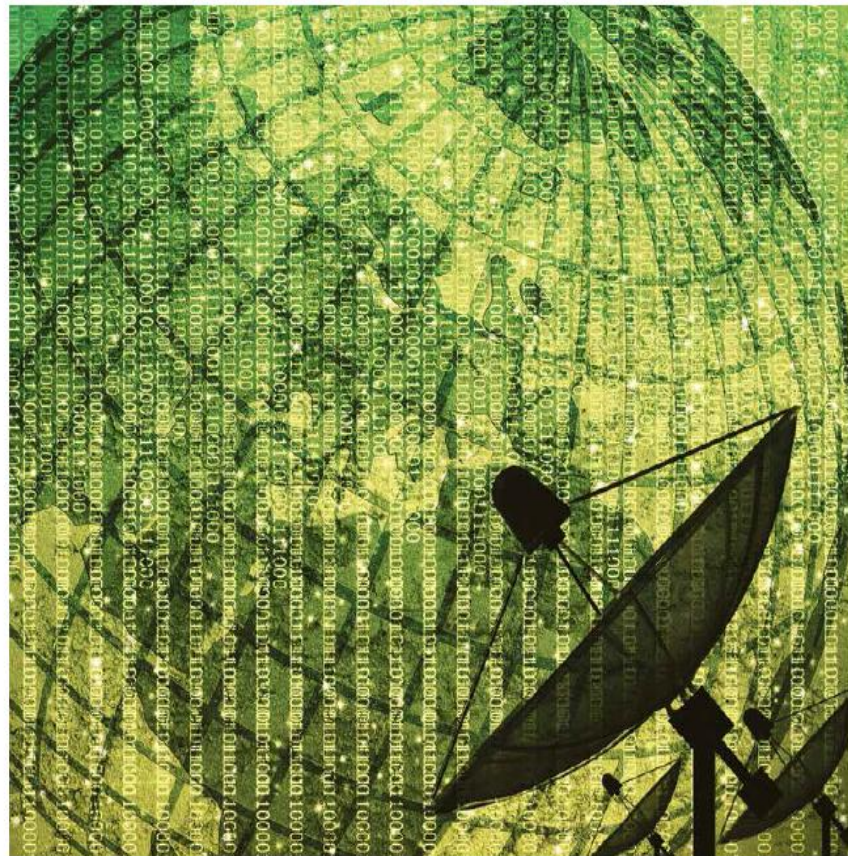
***Introducing
A New Approach:
Applying Privacy by Design
to Surveillance***

www.privacybydesign.ca

Privacy-Protective Surveillance

“As long as the threat of terrorism exists and the global conditions that instantiate those threats continue, effective measures will be needed to counteract terrorism.

At the same time, in order for a free and open society to function properly, privacy and civil liberties must be strongly protected.”



Introducing Privacy-Protective Surveillance: Achieving Privacy *and* Effective Counter-Terrorism

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

Khaled El Emam, Ph.D.
Associate Professor,
University of Ottawa

September 2013

www.privacy.ca

Introducing PPS: Privacy-Protective Surveillance

- A new system of surveillance which enables effective counter-terrorism measures to be pursued – **in a privacy-protective manner**;
- The underling technology builds on Artificial Intelligence, advances in cryptography involving Homomorphic Encryption, and Probabilistic Graphical Models (involving Bayesian Networks).

Privacy-Protective Surveillance – *How Will It Work?*

- Privacy-Protective Surveillance (PPS), begins with a system of feature detection: intelligent, virtual agents are programmed to search databases to detect “significant” information related to potential terrorist activities;
- First, the features/events to be searched for must be identified by intelligence experts in the field;
- Any personal information associated with significant features or events detected after a search will be encrypted;
- No personally identifiable information will remain in plain text;
- A system of public key encryption will be used to encrypt the data, using the court’s public key.

Examples of Features

- FD1: Purchasing fertilizer capable of bomb-making;
- FD2: Accessing a bomb-making website;
- FD3: Transferring money to a “listed” organization;
- FD4: Telephone call to a “listed” individual;
- FD5: Telephone call from a “listed” telephone number.
- FDn: ...

Privacy-Protective Surveillance – *How Will It Work?* (Cont'd)

- A system of “homomorphic encryption” will be used to enable data analysis of the encrypted data, (all analysis will take place on encrypted values – no plain text analysis will occur);
- This will allow for the secure and privacy-protective analysis of the data;
- A probabilistic graphical model will then be constructed on any “significant” data found in order to determine the likelihood of the finding being associated with terrorist activity.

Privacy-Protective Surveillance – *How Will It Work?* (Cont'd)

- The evidence of detected events/features, together with the links and common identities, will function to prune the comprehensive graphical model into a specific model that will serve as the basis for an anonymous Bayesian network to infer the probability of terrorism;
- It is this probability of inference that will, in part, be used by the court to decide whether or not to issue a warrant to enable access to the court's encryption key (to decipher any personally identifiable information).

Highlights

- PPS only collects data considered to be “significant,” as mapped out by intelligence experts;
- “Significant” data is defined as events or features believed to be related to suspicious activity;
- All personally identifiable information related to significant data will be encrypted;
- Data analytics and queries will only be performed on encrypted data in cypher space;
- If an interesting result is obtained, a more targeted request for the raw data that pertains to those results may be made through the courts – a warrant will be required to decrypt the data.

Summary of PPS

- Privacy Protective Surveillance is a positive-sum, “win-win” alternative to current counter-terrorism surveillance systems. It incorporates two primary objectives in its design:
 1. An AI system consisting of feature detection that scans the Web and related databases using a “blind-sight” procedure to detect digital evidence relating to potentially suspicious terrorist activity by some, without infringing on the privacy of unrelated individuals;
 2. A technological infrastructure to ensure that any personally identifying information (“PII”) on unsuspected individuals is not collected and, in those associated with targeted activity, encrypted PII will only be divulged with judicial authorization (a warrant issued by the court).

Concluding Thoughts

- Get smart and lead with *Privacy by Design*;
- Change the paradigm from the dated “zero-sum” to the doubly-enabling “positive-sum;”
- Deliver *both* privacy AND security, or any other functionality, in an empowering “win-win” paradigm – abandon false trade-offs;
- Embed privacy as a core functionality:
the future of privacy may depend on it!

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