Taking SmartData – the Embodiment of Privacy by Design, to Privacy-Protective Surveillance

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario, Canada

Identity, Privacy and Security Institute
University of Toronto
October 28, 2013

Presentation Outline

1. ***Privacy – Essential to Freedom***
2. ***Privacy by Design: The Gold Standard***
3. **SmartData:** ***Privacy by Design 2.0***
4. ***NSA/CSEC State Surveillance***
5. ***Surveillance Technologies and Privacy***
6. ***Privacy-Protective Surveillance, by Design***
7. ***Concluding Thoughts***

Privacy = Freedom

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:

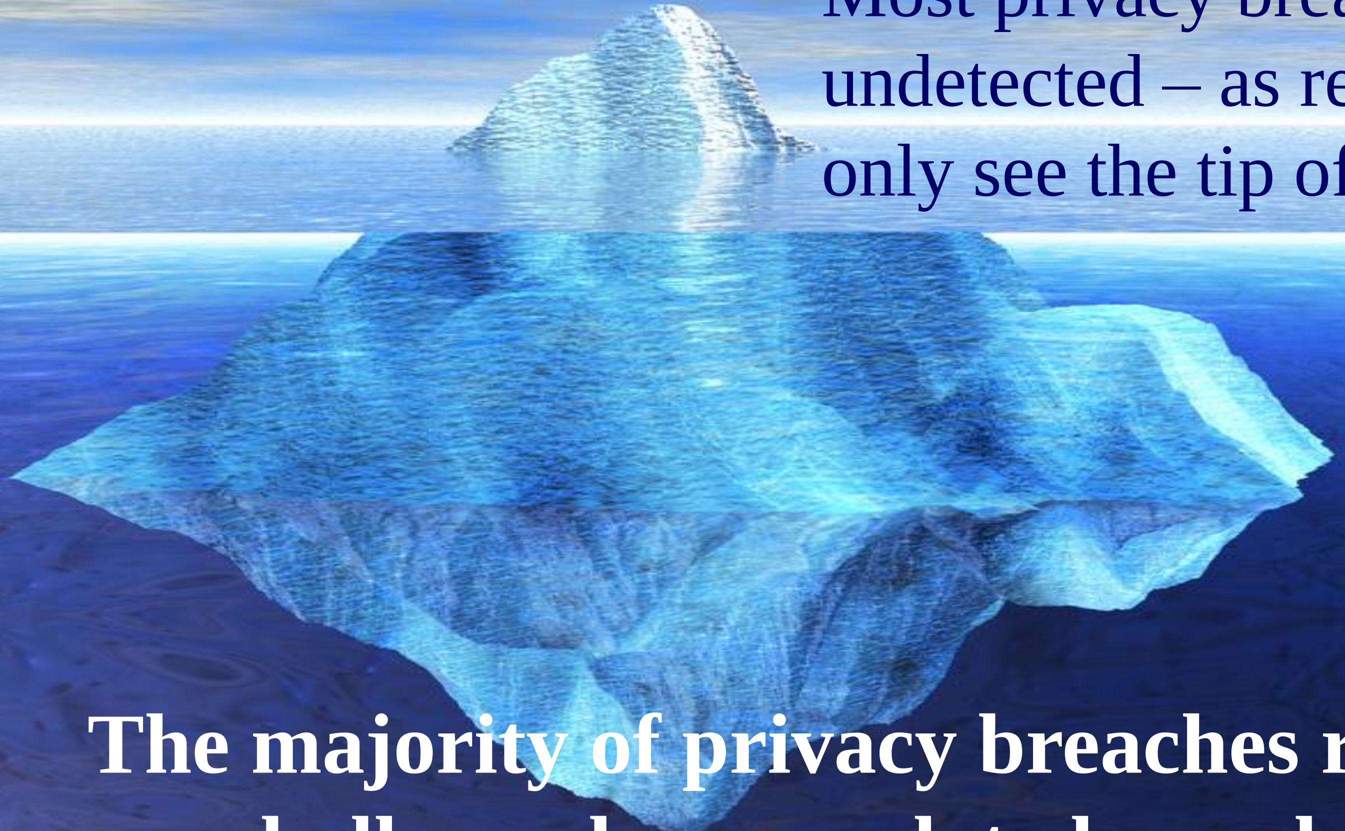
Without privacy, individual human rights, property rights and civil liberties, the conceptual engines of innovation and creativity, could not exist in a meaningful manner;

- 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.

The Decade of Privacy by Design

Why We Need *Privacy by Design*



Most privacy breaches remain undetected – as regulators, we only see the tip of the iceberg

The majority of privacy breaches remain unchallenged, unregulated ... unknown

Regulatory compliance alone, is unsustainable as the sole model for ensuring the future of privacy

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 "vs." with "and"

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**:

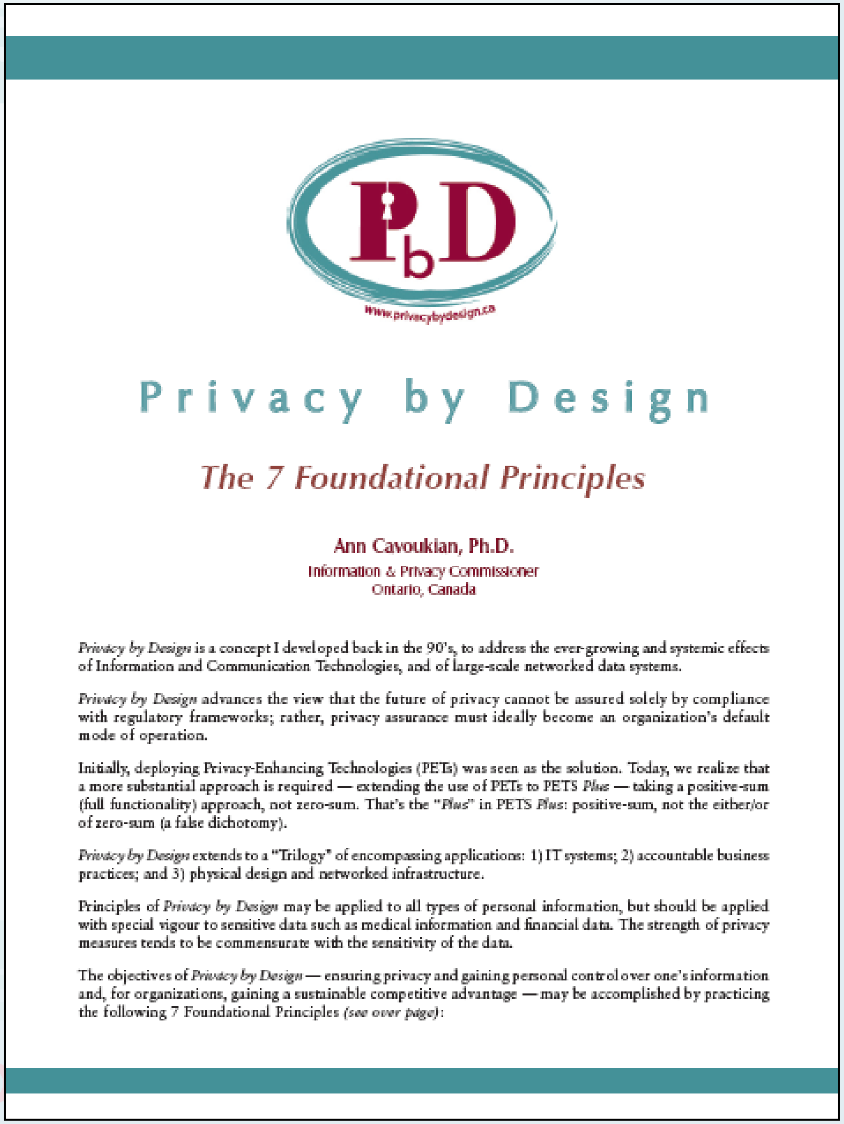
    Full Lifecycle Protection;

6. Visibility **and** Transparency:

    Keep it **Open**;

7. Respect for User Privacy:

    Keep it **User-Centric**.



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

SmartData:
Privacy by Design 2.0

Context is Key

The Next Evolution in Data Protection:

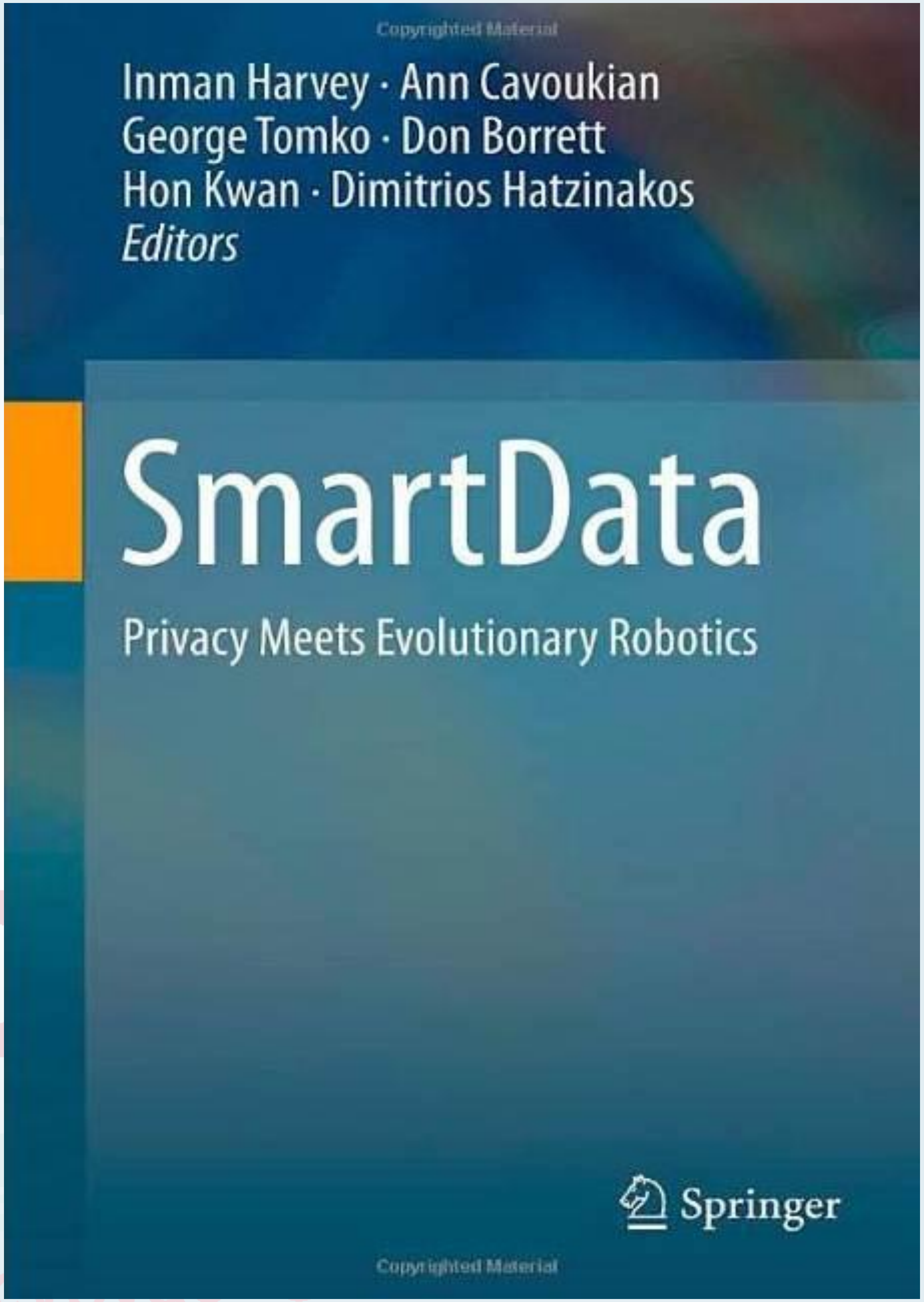
"SmartData"

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

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 .

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

“SmartData empowers personal data by wrapping it in a cloak of intelligence such that it now becomes the individual’s virtual proxy in cyberspace. No longer will personal data be shared or stored in the cloud as merely data, encrypted or otherwise; it will now be stored and shared as a constituent of the binary string specifying the entire SmartData agent.”



Inman Harvey · Ann Cavoukian
George Tomko · Don Borrett
Hon Kwan · Dimitrios Hatzinakos
Editors

SmartData

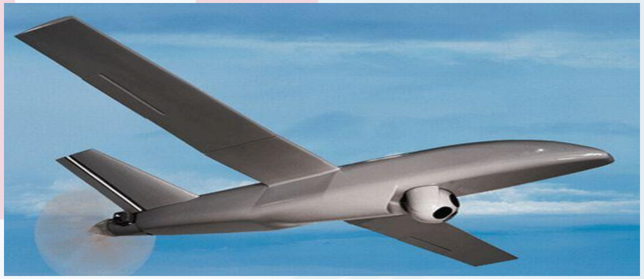
Privacy Meets Evolutionary Robotics

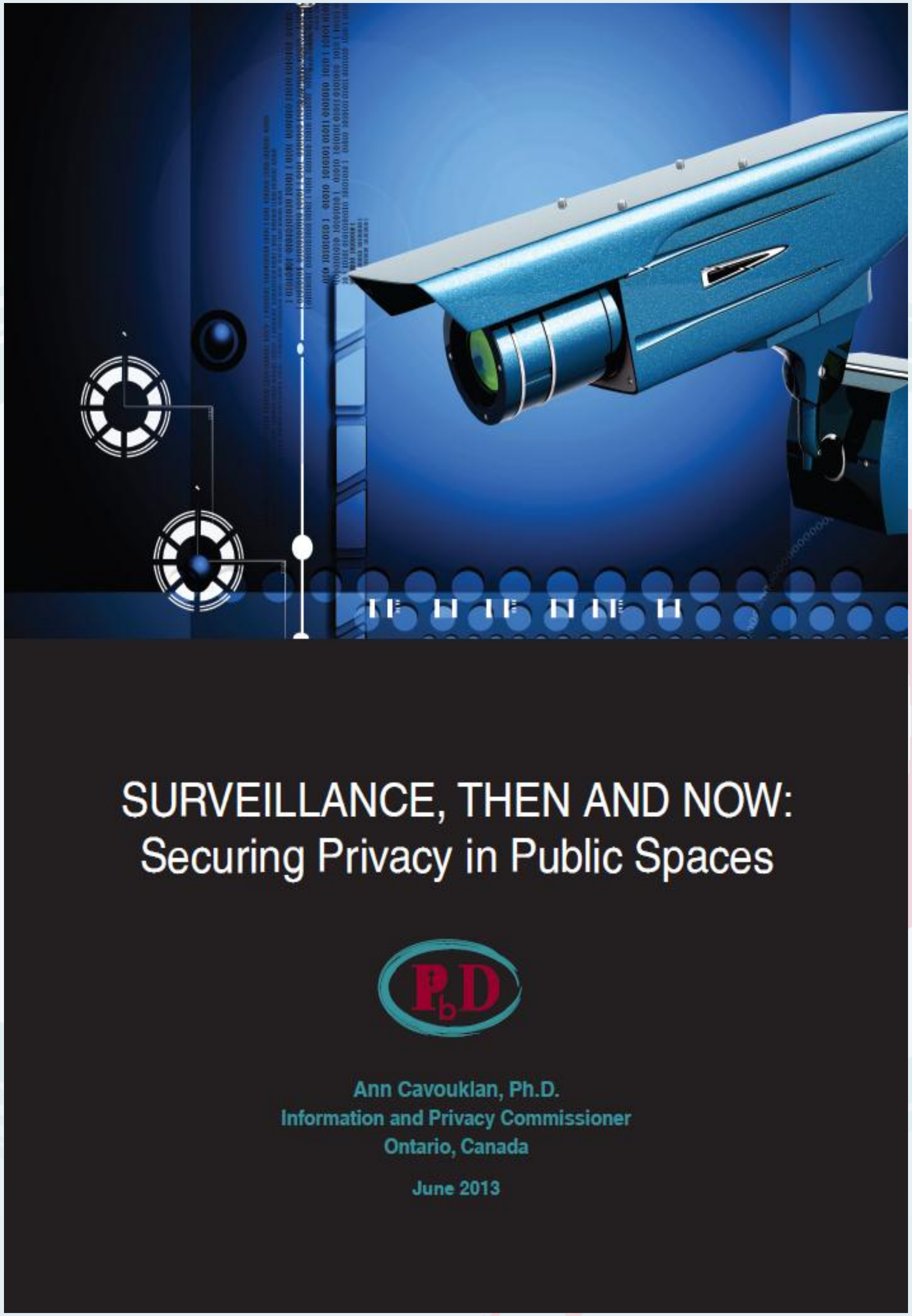
Springer

http://www.springer.com/?SGWID=0-102-24-0-0&searchType=EASY_CDA&queryText=SmartData

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
- Legislation (Bill C-30)





SURVEILLANCE, THEN AND NOW:
Securing Privacy in Public Spaces

PbD

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

June 2013

www.privacybydesign.ca

“There is a fear of becoming a ‘see-through citizen’ in a totalitarian surveillance state.”

— Professor Jesko Kaltenbaek,
Berlin Freie University,
August 24, 2010.

NSA/CSEC and 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, or purpose of their security programs, and in the process, undermined citizen trust in government;
- Transparency in law-making 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 but have 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 Surveillance

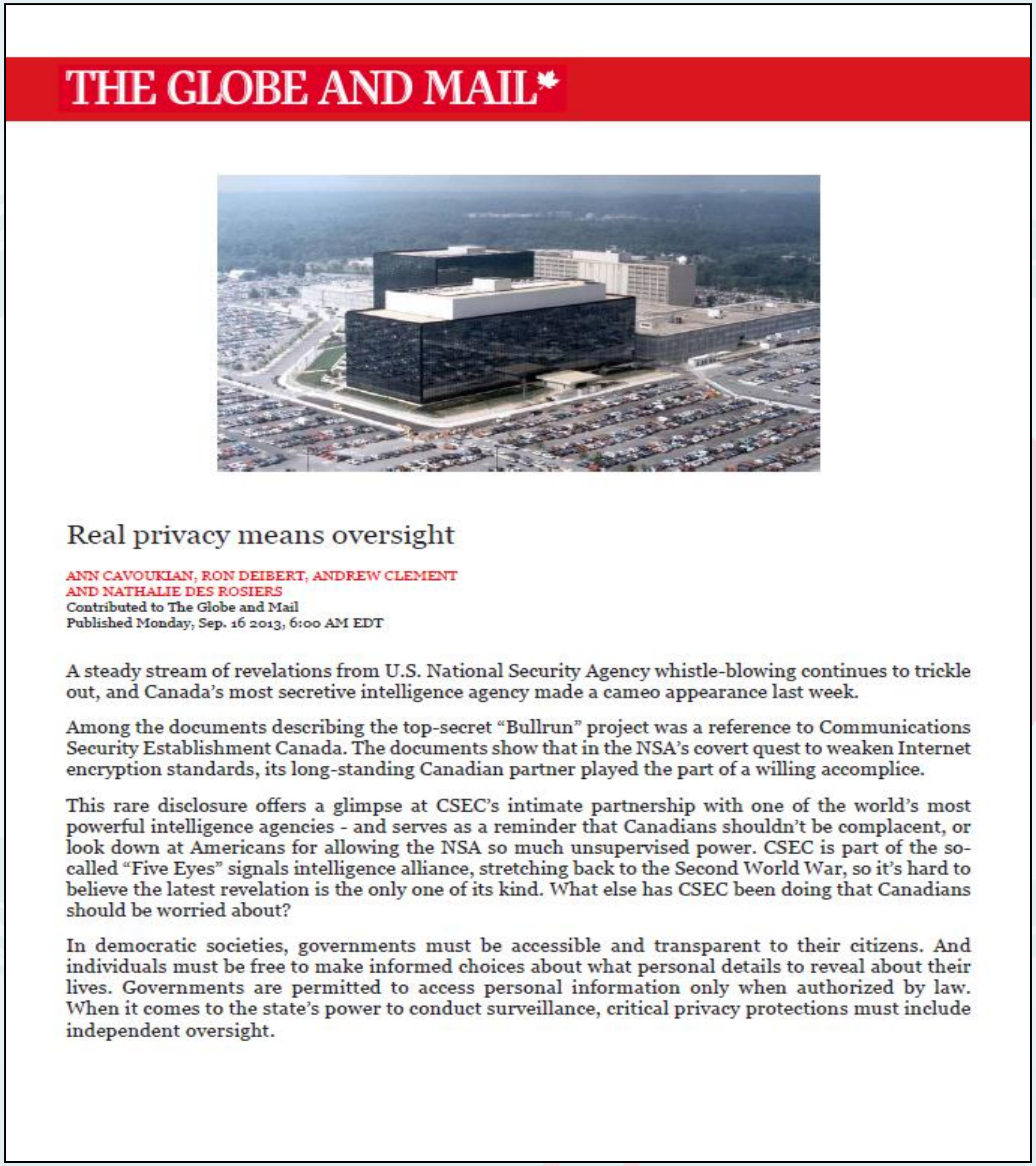
Undermining Encryption

- **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 US and foreign IT industries to covertly influence and/or overtly leverage commercial products’ designs to make them exploitable.

Communications Security Establishment Canada (CSEC)

- It has been 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 standards process for the International Organization for Standardization in 2006, at which time the NSA convinced CSEC into handing over control of the standards process in order to get its preferred encryption code – *with a backdoor* - made a worldwide standard.

Commissioner's Joint Op-Ed



THE GLOBE AND MAIL

Real privacy means oversight

ANN CAVOUKIAN, RON DEIBERT, ANDREW CLEMENT
AND NATHALIE DES ROSIERS
Contributed to The Globe and Mail
Published Monday, Sep. 16 2013, 6:00 AM EDT

A steady stream of revelations from U.S. National Security Agency whistle-blowing continues to trickle out, and Canada's most secretive intelligence agency made a cameo appearance last week.

Among the documents describing the top-secret "Bullrun" project was a reference to Communications Security Establishment Canada. The documents show that in the NSA's covert quest to weaken Internet encryption standards, its long-standing Canadian partner played the part of a willing accomplice.

This rare disclosure offers a glimpse at CSEC's intimate partnership with one of the world's most powerful intelligence agencies - and serves as a reminder that Canadians shouldn't be complacent, or look down at Americans for allowing the NSA so much unsupervised power. CSEC is part of the so-called "Five Eyes" signals intelligence alliance, stretching back to the Second World War, so it's hard to believe the latest revelation is the only one of its kind. What else has CSEC been doing that Canadians should be worried about?

In democratic societies, governments must be accessible and transparent to their citizens. And individuals must be free to make informed choices about what personal details to reveal about their lives. Governments are permitted to access personal information only when authorized by law. When it comes to the state's power to conduct surveillance, critical privacy protections must include independent oversight.

Surveillance Technologies and Privacy

A ‘Wait And See’ Approach is No Longer Sufficient …

- Emerging issues that raise substantial privacy concerns, in addition to CCTV surveillance cameras, include GPS tracking, automatic license plate recognition systems, and more recently, drone-based surveillance;
- The end of “practical obscurity” cannot in any way signal an end to our right to privacy;
- Privacy is being transformed with the rise of *PbD* to **proactively** strengthen the protection of our personal data, and our freedoms.

It is One Thing to Be "Seen" in Public – It is Another to Be Tracked by the State

- Public spaces facilitate a range of vital activities in a democratic society: transportation, recreation, shopping, socializing, and artistic performance;
- **Warrantless** surveillance that facilitates the sustained tracking of people engaging in everyday activities in public spaces is unacceptable in freedom loving countries;
- In Canada's Supreme Court, Justice La Forest referred to such warrantless surveillance as being "unthinkable:" *"It is an unthinkable prospect in a free and open society such as ours."*

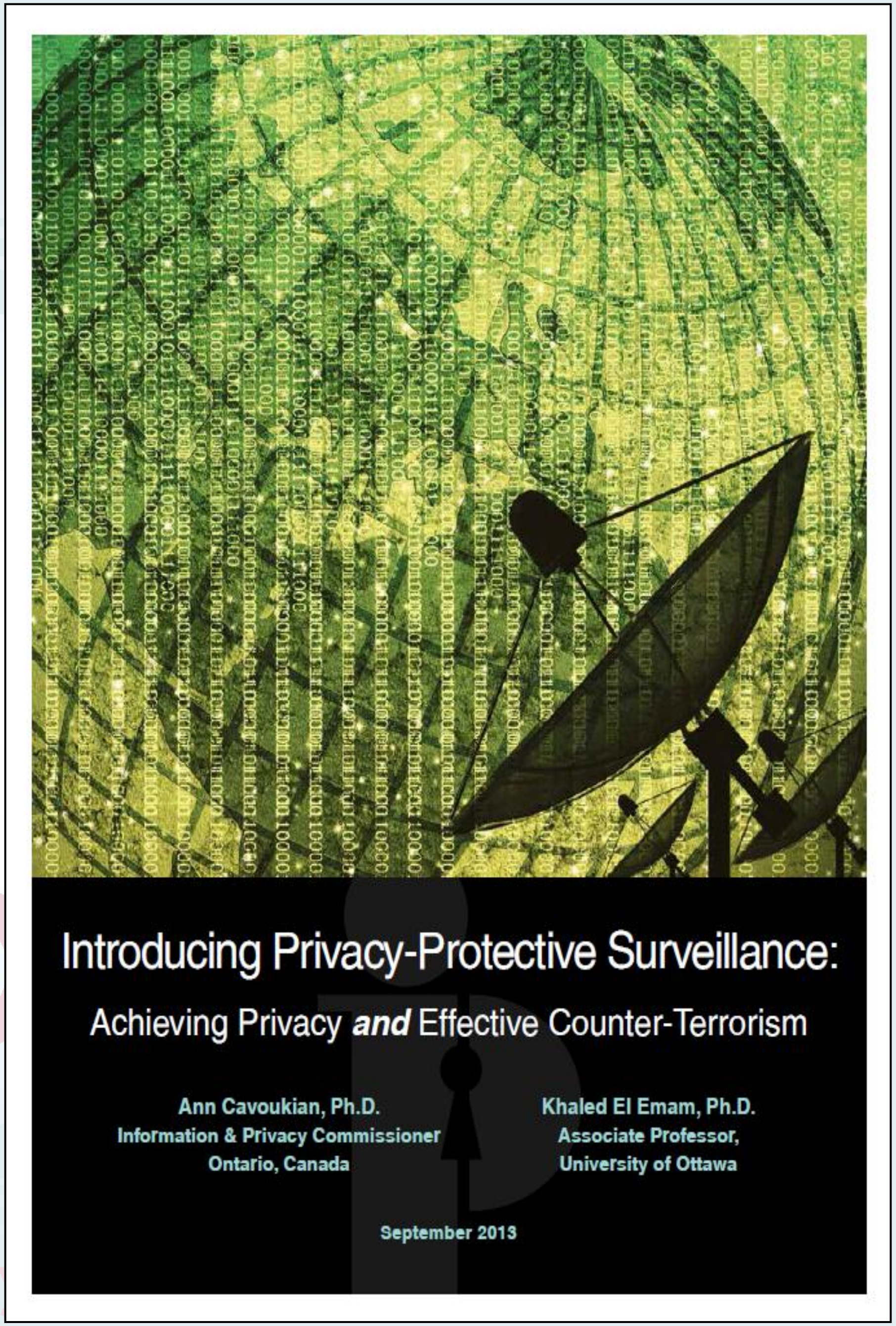
Introducing
A New Approach:

Applying Privacy by Design to Surveillance

Privacy-Protective Surveillance

"As long as the threat of terrorism exist 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

http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1330

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).

PPS: How Does It Work?

1. Intelligence experts will construct a comprehensive graphical model comprising the events or features of interest in determining potential terrorist activity, and the causal or evidentiary relationships between these events/features;
2. AI agents will be developed to search for these events/features in streamed and stored data and, if detected, will encrypt any personal information associated with the event/feature;

Cont'd …

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: …

PPS: How Does It Work? *(Cont’d)*

3. The encryption will be carried out using the “court’s public key” (should the court decide to grant a warrant) and a homomorphic key;
4. The evidence detected by the AI agents will be queried in “cypher space” using partial homomorphic analysis to establish links, and common n-hop identities;

Cont’d …

PPS: How Does It Work? *(Cont'd)*

5. The evidence of detected events and 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, given the evidence;

6. It is this probability of inference that will, in part, be used by the court to decide whether or not to issue a warrant enabling access to the encryption key (to decipher the personal information associated with the individual in question).

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;
- 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).

International Privacy Day: Big Surveillance Demands Big Privacy – Enter Privacy-Protective Surveillance

January 28, 2014

www.realprivacy.ca

Big Surveillance Demands Big Privacy –
Enter Privacy-Protective Surveillance

January 28th, 2014 • 9:00 a.m. to 11:00 a.m.
MaRS Discovery District
101 College Street, Toronto, ON M5G 1L7

Web: www.RealPrivacy.ca • Twitter: @embedprivacy

Concluding Thoughts

- Beware of the steady creep of surveillance technologies, expanding into an ever-growing number of networks and mobile devices;
- Ensure that surveillance is accompanied by privacy measures embedded proactively, by Design, into IT systems and operational processes;
- Surveillance measures by the state must be subject to independent scrutiny, accompanied by prior judicial authorization – transparency and accountability are key;
- 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