

*Preserving Privacy and Freedom,  
Well into the Future – by Design*

**Ann Cavoukian, Ph.D.**

**Information and Privacy Commissioner**

**Ontario, Canada**

*European Commission*

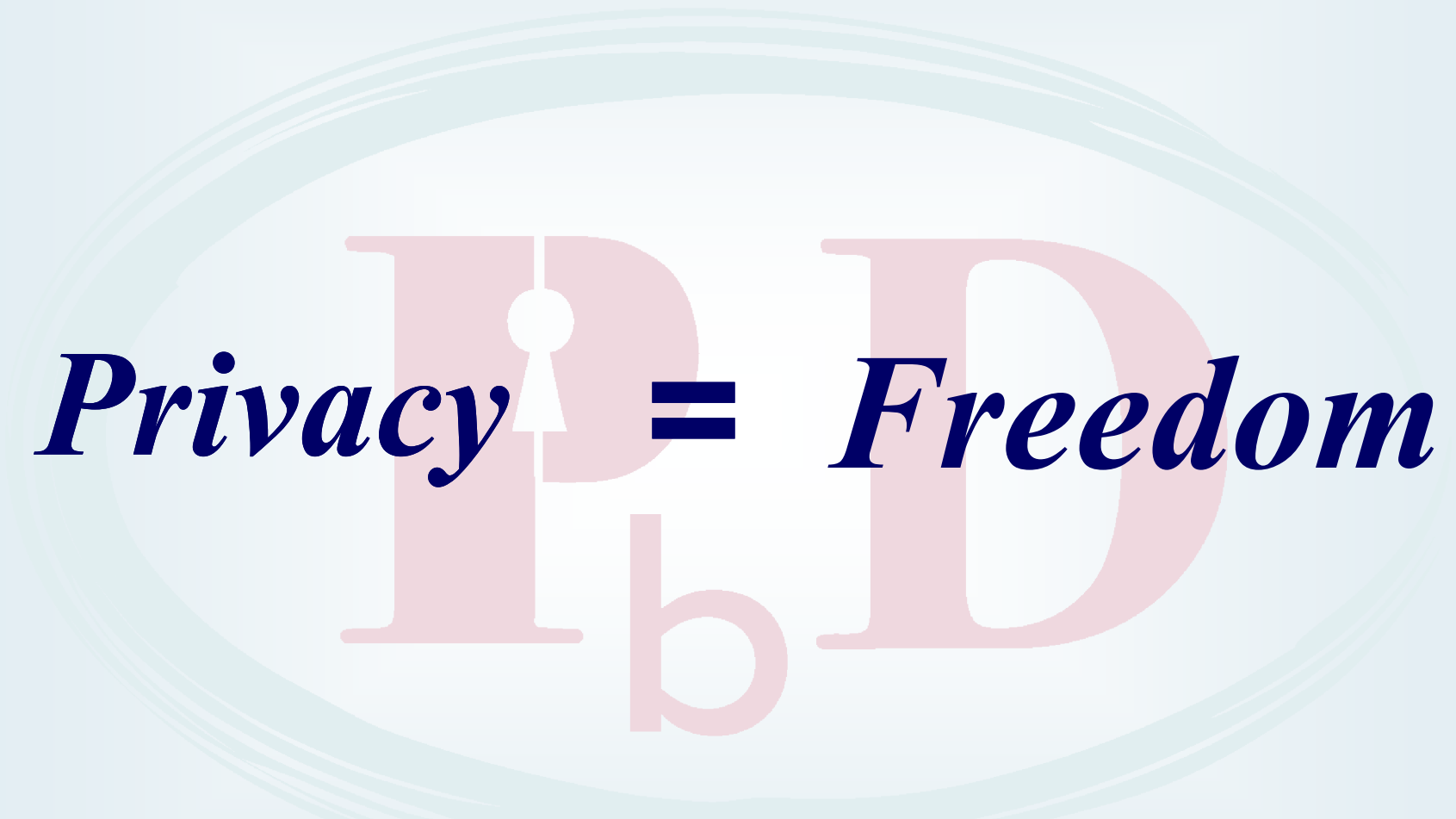
*European Group on Ethics in Science and New Technologies*

*April 16, 2013*

[www.privacybydesign.ca](http://www.privacybydesign.ca)

# Presentation Outline

- 1. Privacy = Freedom*
- 2. An Era of Expanded Surveillance*
- 3. Privacy by Design: The Gold Standard*
- 4. Privacy by Design in Public Safety*
- 5. Data Minimization and De-Identification*
- 6. New White Paper on Surveillance Technologies*
- 7. Concluding Thoughts*



*Privacy* **=** *Freedom*

The central text is overlaid on a large, light blue oval graphic with a double-line border. Behind the text, the letters 'P', 'b', and 'D' are faintly visible in a light red color. The word 'Privacy' is in a dark blue, italicized serif font, followed by an equals sign, and then the word 'Freedom' in the same font style.

[www.privacybydesign.ca](http://www.privacybydesign.ca)

# **Information Privacy/Data Protection Defined**

**Freedom of choice – personal control**

**“Informational self-determination”**

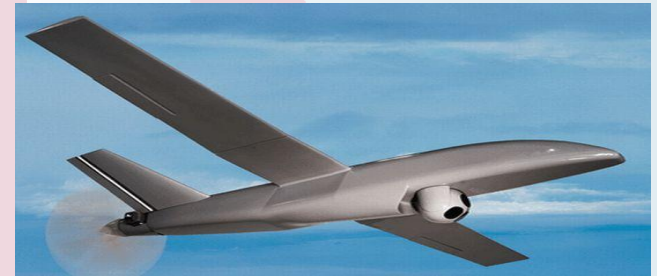
**Fair Information Practices**

**Global Privacy Standard (2006)**

**[www.ipc.on.ca/images/Resources/up-gps.pdf](http://www.ipc.on.ca/images/Resources/up-gps.pdf)**

# *We are Entering an Era of Expanded Surveillance*

- Drones/Unmanned Ariel Vehicles (UAVs)
- Automatic Licence Plate Scanners (ALPs)
- Vehicle Black boxes/GPS
- Video Surveillance (CCTV)
- Biometric Tracking
- Legislation (Bill C-30)
- Big Data/Data Analytics



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

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

*We Need to Change the Paradigm*

*Positive-Sum,*  
*NOT*  
*Zero-Sum*

[www.privacybydesign.ca](http://www.privacybydesign.ca)

# 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 the “vs.” with “and”*



# *Privacy by Design: “Build It In”*

- I first developed the concept of “Privacy by Design” in the 90s, as a response to the growing threats to online privacy that were beginning to emerge, but its need grew dramatically after the tragic events of 9/11;
- “Privacy by Design” seeks to build in privacy – up front, right into the design specifications; into the architecture; embed privacy into the technology used – *bake it in*;
- Data minimization is key: minimize the routine collection and use of personally identifiable information – use encrypted or coded information whenever possible;
- Use privacy-enhancing technologies (PETs) where possible: give people maximum control over their own personal data.

# *The Decade of Privacy by Design*



[www.privacybydesign.ca](http://www.privacybydesign.ca)

# 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*

# *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*):

# *Positive-Sum is Paramount: Achieving Public Safety and Privacy*

- Government and law enforcement agencies frequently require personal information for national security and public safety. However, privacy, liberty and freedom of choice are also essential to the functioning of prosperous and democratic free societies;
- We have shifted our focus from “balance” to taking a positive-sum (win/win) approach in tackling public safety issues;
- Protecting privacy need not stand in the way of public safety – you can do both.

**Abandon Zero-Sum, Simplistic either/or Solutions –  
Positive-Sum is Paramount:  
Achieving Public Safety and Privacy**



November 2012

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



Information and Privacy Commissioner,  
Ontario, Canada

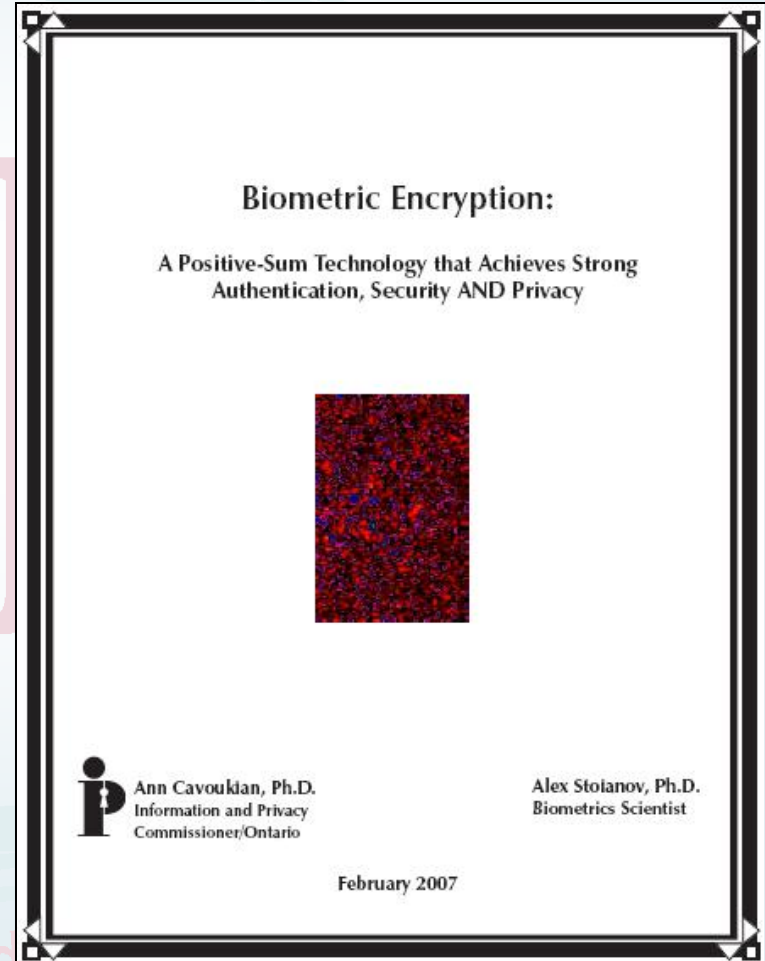
# *Privacy by Design in Public Safety*

- Privacy-Protective Biometrics
- “Surveillance by Design” Legislation
- Data Minimization and De-Identification

# Biometric Encryption:

## *A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*

- Privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of BE, over other biometrics;
- BE technology can overcome the prevailing “zero-sum” paradigm by effectively transforming one’s biometric into a private key.



# Failing to Adopt *Privacy by Design* in Public Safety

- Failure to adopt a *PbD* approach has led to an erosion of public confidence in law enforcement initiatives, for example in the mandatory collection of personal information in the context of telecommunications and policing;
- It is critical to bake privacy into a program, policy, or legislative initiative, right from the beginning.



# Beware of *Surveillance by Design*

- **Summer, 2011** – One of the greatest threats to privacy actually materialized from within my own federal government – *Bill C-30* – which would have enabled *warrantless access* by law enforcement;
- Throughout our opposition to *Bill C-30*, I referred to the proposed warrantless access as a system of “*Surveillance by Design.*”

# Commissioner's Op-Ed: [Un]Lawful Access


nationalpost.com | financialpost.com | Today's Paper | Delivery | Contact | Digital Paper | Sign In | Register Today

## NATIONAL POST

National Post | Full Comment | Canada | Environment | Letters | Policy | Pop Culture | Social Issues | U.S. Politics | World Politics

### FULLCOMMENT

#### Privacy Commissioner Ann Cavoukian: Privacy invasion shouldn't be 'lawful'



We should not allow government to violate our right to be secure from unreasonable state surveillance. foto

National Post Oct 31, 2011 — 7:30 AM ET | Last Updated: Oct 27, 2011 4:32 PM ET

**By Ann Cavoukian**

I must add my voice to the growing dismay regarding the impact of impending "lawful access" legislation in this country. In my view, it is highly misleading to call it "lawful." Let's call it what it is — a system of expanded surveillance.

At issue is the anticipated re-introduction of a trio of federal bills that will provide police with much greater ability to access and track information, via the communications technologies we use every day, such as the Internet, smart phones and other mobile devices. I have no doubt that, collectively, the legislation will substantially diminish the privacy rights of Ontarians and Canadians as a whole.

Let's take a brief look at the surveillance bills, which were introduced prior to the last election:

- Bill C-50 would make it easier for the police to obtain judicial approval of multiple intercept and tracking warrants and production orders, to access and track e-communications.
- Bill C-51 would give the police new powers to obtain court orders for remote live tracking, as well as suspicion-based orders requiring telecommunication service providers and other companies to preserve and turn over data of interest to the police.
- Bill C-52 would require telecommunication service providers to build and maintain intercept capability into their networks for use by law enforcement, and gives the police warrantless power to access subscriber information.

I well understand the attraction for law enforcement officials — the increased ability to access and track our e-communications, with reduced judicial scrutiny, would put a treasure trove of new information at their fingertips.

However, we must be extremely careful not to allow the admitted investigative needs of police forces to interfere with or violate our constitutional right to be secure from unreasonable state surveillance. The proposed surveillance powers come at the expense of the necessary privacy safeguards guaranteed under the Charter of Rights and Freedoms. The federal government must be persuaded to acknowledge the sensitivity of traffic data, stored data and tracking data, and strongly urged to re-draft the bills. For a start, the proposal for warrantless access to subscriber information is untenable and should be withdrawn. If special access to subscriber information is considered to be absolutely necessary, it must take place under a court-supervised regime.

The government needs to step back and consider all of these implications. A comprehensive cost-benefit analysis should precede the entrenchment of so many significant public policy decisions. Public Parliamentary hearings must also be scheduled to ensure that civil society, as well as the telecom industry, has a full opportunity to provide input.

Canadians must press the federal government to publicly commit to enacting much-needed oversight legislation in tandem with any expansive surveillance measures. Intrusive proposals require, at the very least, matching legislative safeguards. The courts, affected individuals, future Parliaments and the public must be well informed about the scope, effectiveness and damaging negative effects of such intrusive powers.

We can, and must, have both greater security and privacy, in unison. It cannot be one at the expense of the other. The true value of privacy must be recognized in any effort to modernize law enforcement powers. Imposing a mandatory surveillance regime on the public and its telecom service providers must not go forward without strong safeguards to protect the future of our fundamental freedoms.

National Post

**Ann Cavoukian is the Information Privacy Commissioner of Ontario.**



Information and Privacy Commissioner of Ontario  
2 Bloor Street East, Suite 1400  
Toronto, ON M4W 1A8  
CANADA

TEL: 416-326-3333  
Toll-free: 1-800-387-0073  
Fax: 416-326-9195  
Email: [info@ipc.on.ca](mailto:info@ipc.on.ca)  
Website: [www.ipc.on.ca](http://www.ipc.on.ca)

Give Me RealPrivacy

NOT

PRIVACY THEATRE

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

[www.RealPrivacy.ca](http://www.RealPrivacy.ca)

# Demise of Bill C-30



## Harper government kills controversial Internet surveillance bill

JOHN IBBITSON

Ottawa — The Globe and Mail

Published Monday, Feb. 11 2013, 3:42 PM EST

Last updated Tuesday, Feb. 12 2013, 9:57 AM EST



695



457



224



14



29



Print / License

AA

The Harper government will not resurrect its controversial Internet surveillance bill, and will not introduce new legislation to monitor the activities of people on the web.

The bill, which excited outrage over possible privacy violations on the Internet, marks a legislative failure for the Harper majority government.

### MORE RELATED TO THIS STORY

- **JOHN IBBITSON** Can Conservatives resurrect the Internet surveillance bill?
- **SURVEILLANCE** Can Internet snooping protect us, or do criminals just get used to it?
- Telcos in talks with Ottawa to shape Internet 'spy' bill: documents



VIDEO

Video: Government

"We've listened to the concerns of Canadians," Justice Minister Rob Nicholson told reporters outside the House of Commons on Monday.

He said that "we will not be proceeding with Bill C-30. And any attempts to modernize the criminal code will not contain warrantless



***Data Minimization  
and  
De-Identification***

[www.privacybydesign.ca](http://www.privacybydesign.ca)

# Data Minimization and De-Identification

- Data minimization and de-identification are the most important safeguards in protecting personal data, including for purposes of research, data analytics and Big Data;

# Big Privacy – Radical Control

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

**Context is Key!**

[www.privacybydesign.ca](http://www.privacybydesign.ca)

# 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



# Data Minimization: Record Linkages

- Dr. El Emam has also developed a protocol for securely linking databases without sharing any identifying information;
- The protocol uses homomorphic encryption to identify and locate records relating to an individual, existing in multiple datasets;
- This involves encrypting personal identifiers in each dataset and comparing only the encrypted identifiers, using mathematical operations, resulting in a list of matched records, without revealing any personal identifiers;
- The protocol promotes compliance with existing prohibition in *PHIPA* by allowing linkages of datasets without the disclosure of any identifying information – a win/win solution – positive-sum!

# Homomorphic Encryption

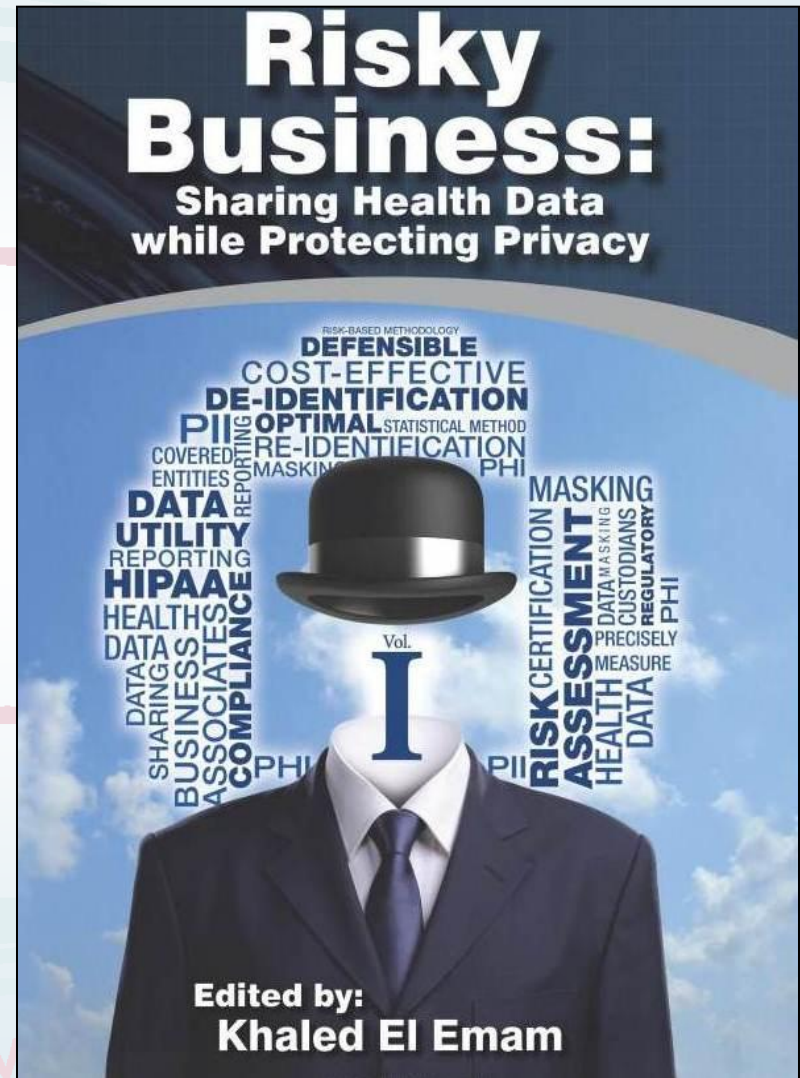
- A form of encryption that allows computations to be carried out on encrypted data, to obtain encrypted results;
- “Homomorphic” describes the transformation of one data set into another while preserving relationships between data elements in both sets;
- Homomorphic encryption allows you to make computations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

# *Risky Business:*

## *Sharing Health Data While Protecting Privacy*

*“By adopting responsible data sharing practices, researchers, companies and the general public can gain the benefits and the promise of big data analytics without sacrificing personal privacy or infringing upon law or regulation.”*

[www.privacyby](http://www.privacyby)



<http://amzn.to/15QvatG>

# IPC De-identification Centre

- The IPC launched a new **De-identification Centre** which aims to foster proper de-identification techniques and best practices, to demonstrate the necessity of de-identification;
- We must spread the word on the importance of de-identification – a key method to protect privacy *and* enable innovation;
- I invite you to participate in our De-Identification Centre: Submit a 350 – 500 word blog post to [pbd@ipc.on.ca](mailto:pbd@ipc.on.ca) – spark conversation on best practices or other issues related to de-identification.



***New IPC White Paper***

[www.privacybydesign.ca](http://www.privacybydesign.ca)

# A Proactive Approach to Overseeing New Surveillance Technologies: Privacy is A Must

- New white paper:
- Securing privacy in public: overseeing the use of drones and other forms of domestic surveillance.




# A ‘Wait And See’ Approach is No Longer Sufficient ...

- Emerging issues that raise substantial privacy concerns include automatic license plate recognition systems, GPS tracking, and 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.

# **It is One Thing to Be Seen in Public – It is Another to Be Tracked by the State in Free and Democratic Societies – Say No!**

- 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 Canada’s Supreme Court, Justice La Forest referred to such warrantless surveillance as “unthinkable:”  
*“It is an unthinkable prospect in a free and open society such as ours.”*





***SmartData***

[www.privacybydesign.ca](http://www.privacybydesign.ca)

# 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.

# 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!

# Concluding Thoughts

- Lead proactively with *Privacy by Design* in matters relating to law enforcement and public safety;
- Warrantless surveillance will lead to intense scrutiny from the public, the media, lawmakers, courts and regulators concerned about protecting privacy;
- We have demonstrated that it is possible to bring together divergent views to achieve public safety objectives, while at the same time, minimize the impact on privacy;
- If you don't practice *Privacy by Design*, you may end up with *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](http://www.ipc.on.ca)**

**E-mail: [info@ipc.on.ca](mailto:info@ipc.on.ca)**

**For more information on *Privacy by Design*,  
please visit: [www.privacybydesign.ca](http://www.privacybydesign.ca)**