Data, Data Everywhere –
The Need for Big Privacy in a World of Big Data

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario, Canada

15th Annual Privacy and Security Conference
February 6, 2014

PbD
www.privacybydesign.ca

Presentation Outline

1. *Privacy is Essential to Freedom*
2. *NSA/CSEC Surveillance*
3. *Privacy by Design: The Gold Standard*
4. *Operationalizing Privacy by Design*
5. *Big Data Needs Big Privacy*
6. *Personal Data Ecosystem*
7. *Concluding Thoughts*

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.

PbD
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.

PbD
www.privacybydesign.ca

NSA/CSEC Surveillance

Edward Snowden Revelations

- Edward Snowden's revelations are having 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 free society, 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, but also set a chill at the heart of the North American Internet economy.

Recommendations for the NSA's Bulk Telephony Metadata Program

Recommendation	The President's Review Group on Intelligence and Communications Technologies	The Privacy and Civil Liberties Oversight Board
End the program	Agreed; However, if it is determined that the collection is necessary, a third party should hold the data, not the government	Agreed (per a majority of the board)
Service providers should be authorized to disclose statistical information regarding FISA Court orders	Agreed	Agreed
Create a new independent advocate to appear before the FISA Court	A "Public Interest Advocate" should be established to represent privacy and civil liberties interests before the court on the initiative of the advocate	Create a pool of "Special Advocates" to appear in "important cases" at the court's discretion
More FISA Court decisions should be declassified	Agreed	Agreed

PbD
www.privacybydesign.ca

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

CSEC's Collection of Canadians' Data "Incidental"

- The federal government is defending the CSEC in a lawsuit filed by the B.C. Civil Liberties Association (BCCLA) insisting its spying activities are legal and essential to protecting Canadians;
- The BCCLA's lawsuit objects to instances in which foreign spying sweeps up Canadians' communications, as well as the collection of electronic metadata which violates the charter rights of Canadians;
- The federal government claims that it is not possible to predict whether spying will inadvertently capture Canadians' private information;
- The government further claims that CSEC's collection of metadata has prevented attacks against Canadians – ***though it does not offer any specifics to back up that claim.***

— James Keller,
CSEC's collection of Canadians' data "incidental",
CTV News, January 24, 2014

"Shameful Absence" of Transparency in Canada

"The U.S. reaction stands in stark contrast to the situation in Canada. ***The shameful Canadian surveillance silence*** *– from both government and the telecom sector – must end with an open conversation about Canadian activities and whether current law strikes the right balance."*

— Professor Michael Geist,
The Shameful Canadian Silence on Surveillance,
January 17, 2014.

"We should hang our heads in shame at the current absence of a real debate on 21st century espionage in Canada."

— Professor Wesley Wark,
Opinion: A Discussion Canada Needs,
Ottawa Citizen, January 22, 2014.

PbD
www.privacybydesign.ca

CBC – The National
CSEC Eavesdropping at Major Canadian Airport

- **January 30, 2014** – CSEC used information from the free Wi-Fi spots at a major Canadian airport to track thousands of ordinary airline passengers and visitors for up to two weeks after they left the terminal;
- CSEC was provided with information on everyone who used the airport's Wi-Fi system over a two-week period, including many Canadians whose smartphone signals were intercepted without their knowledge;
- CSEC was also able to track travelers and visitors for two weeks as their wireless devices showed up in other Wi-Fi zones or hot spots around Toronto and other points in Canada and the U.S.

CBC – The National
CSEC Eavesdropping at Major Canadian Airport

- **Professor Ron Deibert** – *"I can't see any circumstance in which this would not be unlawful, under current Canadian law, under our Charter, under CSEC's mandates … I cannot imagine any circumstances that would have convinced a judge to authorize it."*
- **Professor Wesley Wark** – *"I cannot see any way in which it fits CSEC's legal mandate … outside its mandate and even the law, you are in a situation for democracy where you simply don't want to be."*
- **Chief of CSEC, John Forster** – *"We do not target Canadians at home or abroad in our foreign intelligence activities, nor do we target anyone in Canada. In fact, it's prohibited by law.*

— CBC – The National,
January 30, 2014.

Global Government Surveillance Reform

The undersigned companies believe that it is time for the world's governments to address the practices and laws regulating government surveillance of individuals and access to their information.

While the undersigned companies understand that governments need to take action to protect their citizens' safety and security, we strongly believe that current laws and practices need to be reformed.

Consistent with established global norms of free expression and privacy and with the goals of ensuring that government law enforcement and intelligence efforts are rule-bound, narrowly tailored, transparent, and subject to oversight, we hereby call on governments to endorse the following principles and enact reforms that would put these principles into action.

Aol. facebook Google LinkedIn Microsoft YAHOO!

It's Time for a Change:

Change the Paradigm to Positive-Sum,

NOT

Zero-Sum

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

Change the paradigm
from the dated 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 35 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*

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

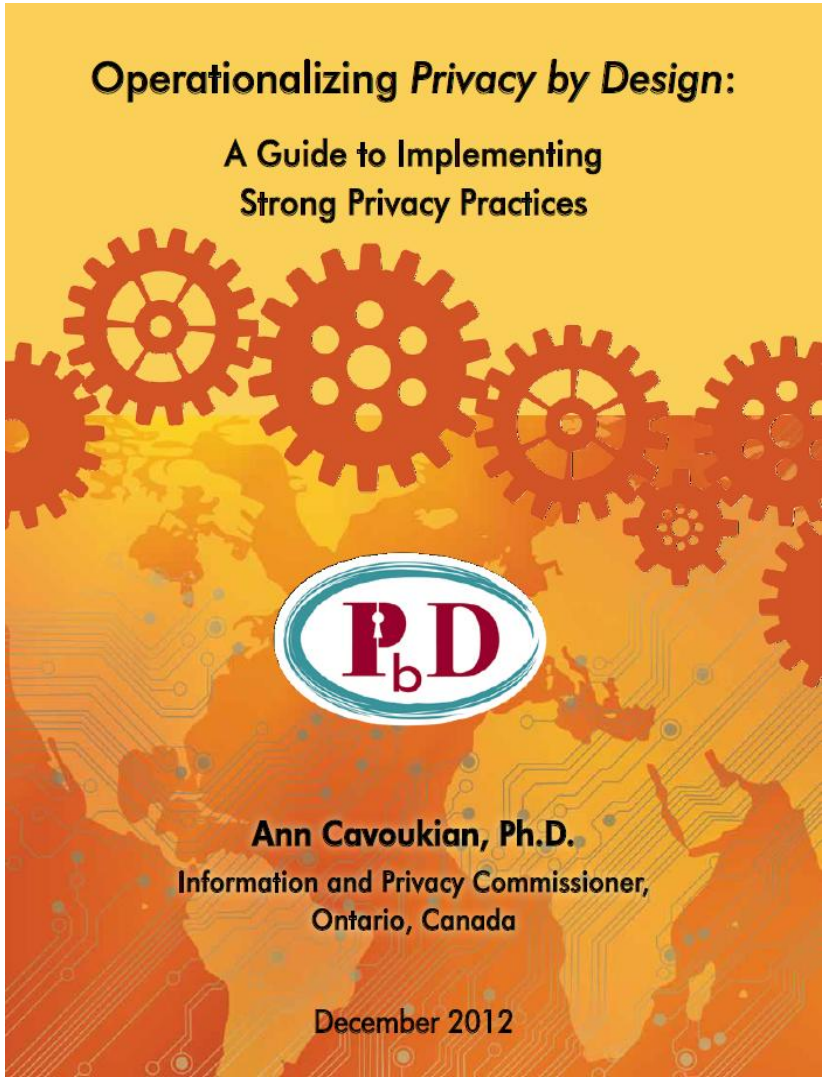
www.privacybydesign.ca

Operationalizing Privacy by Design

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

“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.*

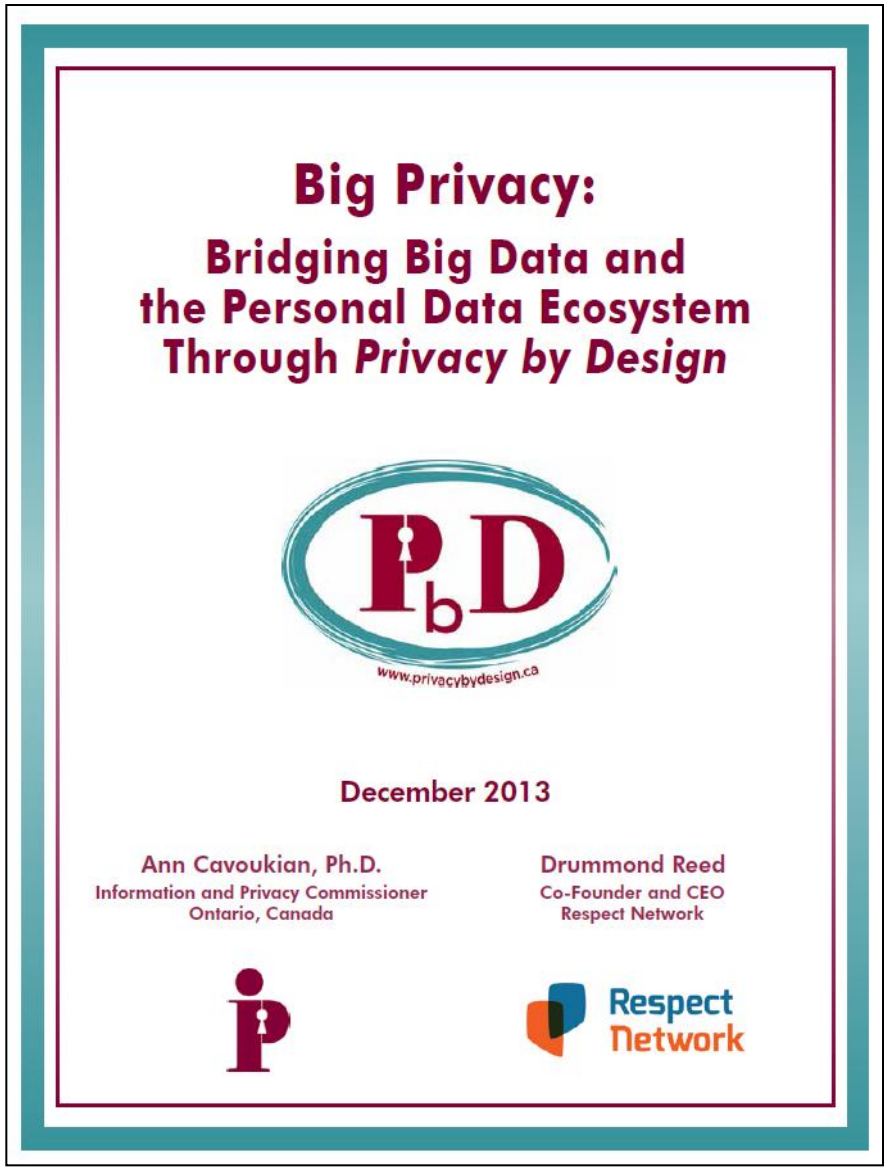
PbD
www.privacybydesign.ca

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).

"… 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 – Personal Control

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

Context is key!

Viktor Mayer-Schönberger:
Forget Notice and Choice, Let's Regulate Use

- **December, 2013** – in his keynote at the IAPP Data Protection Congress in Brussels, Viktor Mayer-Schönberger argued:
  - Informational self-determination "has turned into a formality devoid of meaning and import;"
  - Abandon the notice and choice (consent) model in favour of allowing organizations to determine the appropriate secondary uses of personal data;
  - Regulators expected to assess the harms and offer redress.

I disagree with all of the above

PbD
www.privacybydesign.ca

Our Blog Post
January 8, 2014

"Consent and Personal Control Are Not Things of the Past"

- My colleagues, Commissioner Alexander Dix and Professor Khaled El Emam and I presented a blog post challenging the arguments presented by Victor Mayer-Schönberger in "Data Protection Principles for the 21st Century;"
- We refuted the view that consent and personal control of one's data by data subjects was a thing of the past — **it is not**;
  (We will be releasing a white paper shortly supporting our views);
- Further, in the wake of Edward Snowden's revelations, we are witnessing the opposite: a resurgence of interest in strengthening personal privacy;
- To suggest that Big Data's entry into the world of personal data must inevitably lead to the obliteration of Fair Information Practices is off-base.

PbD
www.privacybydesign.ca

“I Never Said That” – Viktor Mayer-Schönberger

- **January 14, 2014** – Mr. Mayer-Schönberger responded to our blog post by stating that we had either misunderstood him or we had not listened to what he said;
- He stated that his argument was not information privacy as a value, but the mechanisms we currently employ to protect our privacy;
- Further he said we had misunderstood his argument that the core mechanism used to protect information privacy, namely consent at the time of collection, was in practice not effective;
- He further defended his claim that needing more accountability of data users does not imply that data subject’s consent is no longer important.

So Glad You Didn't Say That! – Commissioner Cavoukian

- **January 16, 2104** – I responded to Mr. Mayer-Schönberger by reaffirming that the changes to privacy protection proposed in his papers included removing purpose specification and leaving the decision to obtain consent to the discretion of the organization;
- The acceptable determination of secondary uses of the data would be left up to the company or government involved – not the data subject;
- Since the OECD principles are interrelated (and were re-affirmed in July, 2013), removing such fundamental concepts as purpose specification and use limitation would unhinge the rest of the principles.

PbD
www.privacybydesign.ca

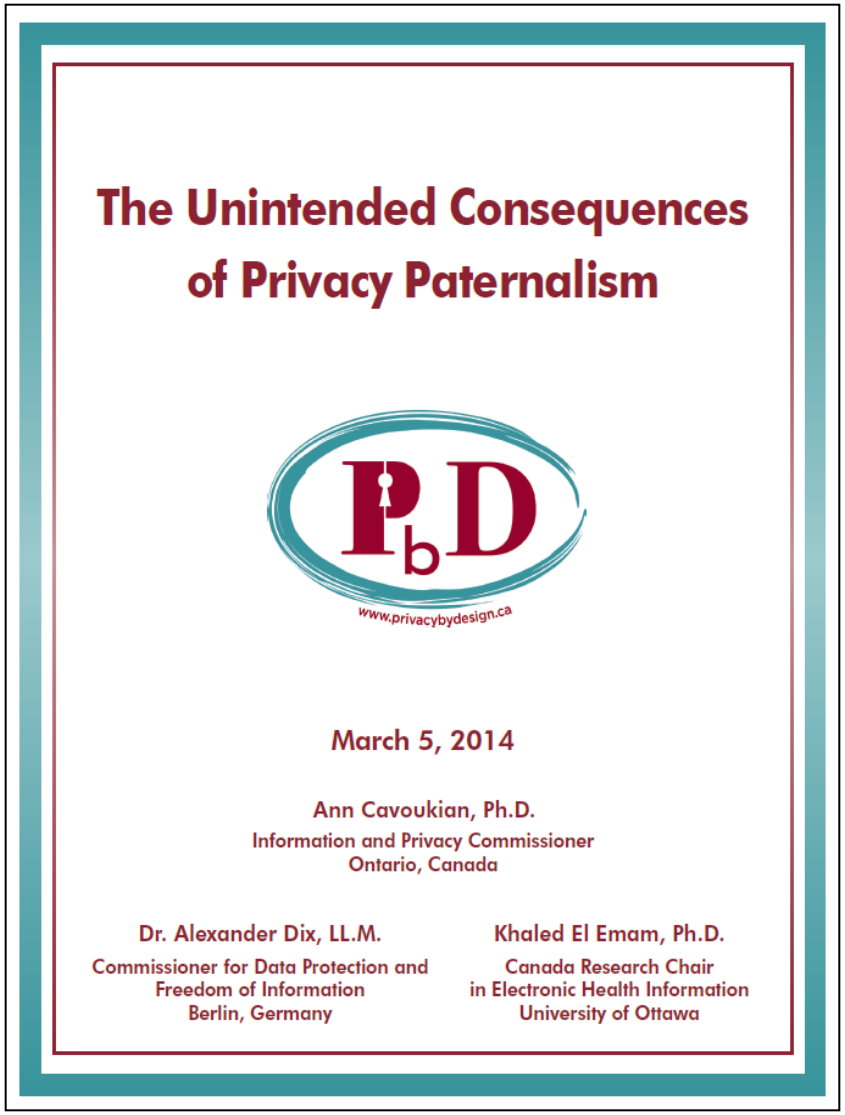
Accountability Model Not Enough

- Mayer-Schönberger suggested that in place of consent and purpose specification, an accountability model in which reasonable safeguards of use and regulatory oversight, rather than consent, regulate the use of personal information;
- I am in favour of responsible data use and accountability but not for eliminating the data subject from the picture, or making the necessary determinations relating to the uses of one's personally identifiable information;
- This is a negative-sum, lose/lose proposition.

Lose/Lose – Negative Sum

- The Accountability Model is the antithesis of *Privacy by Design* (proactive privacy protection) in terms of allowing privacy harms to develop and then, after-the-fact, offering systems of redress – too little, too late;
- We also cannot expect regulators to effectively take this on; with the massive growth in online connectivity and ubiquitous computing, our offices and resources are already stretched to the limit, with no additional resources being allocated for such additional enforcement.

Coming on March 5, 2014



PbD
www.privacybydesign.ca

Protect Privacy with De-Identified Data

- De-identification and data minimization are among the most important safeguards in protecting personal information;
- You should not collect, use or disclose personal information if other data (i.e., de-identified, encrypted, aggregated or obfuscated) will serve the purpose;
- The use of strong de-identification, aggregation and encryption techniques are absolutely critical, and readily available.

“Companies Should be Allowed to Innovate with De-identified Data”

“Re-identification concerns are over-stated … anonymized data can, in many circumstances, be used without fear of re-identification .”

— Information Technology and Innovation Foundation,
January 17, 2104

Concluding Thoughts

- Beware of the steady creep of surveillance technologies, expanding into a growing number of devices;
- Ensure that surveillance is accompanied by privacy measures, embedded by design, into IT systems, business practices and operational processes;
- Surveillance measures by the state must be accompanied by judicial authorization – a court order/warrant;
- 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