Big Data Calls for Big Privacy – Not Only Big Promises

January 24, 2014

www.privacybydesign.ca

Speakers

Dr. Ann Cavoukian
Information and Privacy Commissioner
Ontario, Canada

Dr. Alexander Dix
Commissioner for Data Protection and Freedom of Information
Berlin, Germany

Dr. Khaled El Emam
Associate Professor
Faculty of Medicine
University of Ottawa

Nuala O'Connor
President & CEO
Center for Democracy & Technology

PbD
www.privacybydesign.ca

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

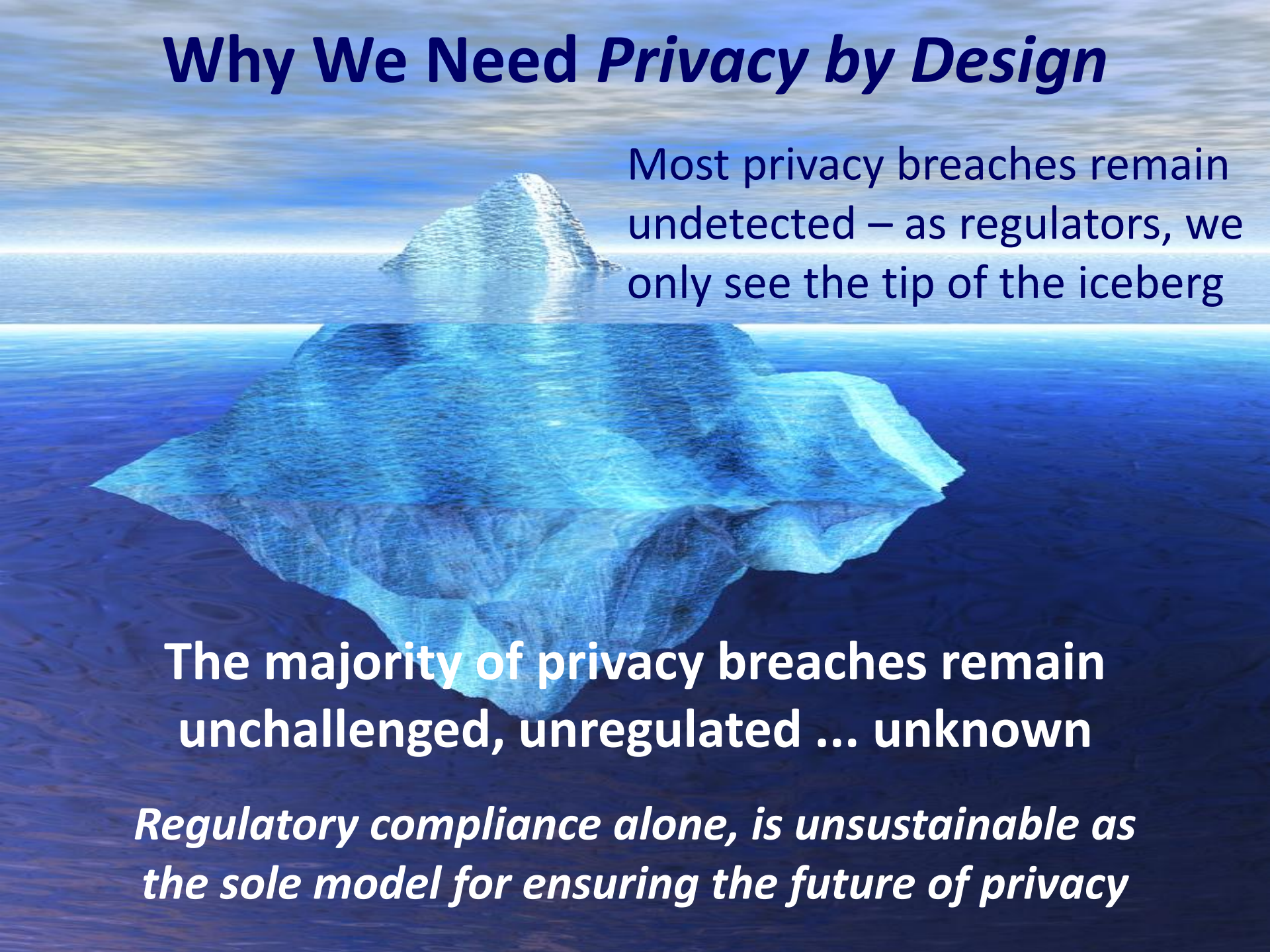
Accountability Model Alone

- 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, in terms of 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.

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

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'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

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 Does *NOT* Stifle Innovation – It Drives 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, Big Data ***and*** privacy may be achieved – we need a new playbook!

PbD
www.privacybydesign.ca

Innovate 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 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

Personal Data Ecosystem

- 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 and organizations 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, allowing far greater control over one's data, and enabling positive returns on its use(s), decided by the data subject;
- ***Context is Key!*** The data subject is the one who is most knowledgeable of the context involved.

PbD
www.privacybydesign.ca

Summary

- Purpose Specification, Collection and Use Limitation are critical to privacy protection;
- A “trust me” model, allowing data users to determine appropriate secondary uses, is doomed to fail;
- Reactive “zero-sum” systems that allow privacy harms to develop are old school; proactive positive-sum models represent the future;
- Regulators are already stretched to the limit, with no additional resources being allocated;
- Get smart – lead with *Privacy by Design* – prevent privacy harms from arising … avoid the fall-out!

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