

***A Time for Innovation:
A Time for Privacy by Design***

Ann Cavoukian, Ph.D.

**Information and Privacy Commissioner
Ontario, Canada**

Economic Club of Canada

May 12, 2010



**P
b
D**

www.privacybydesign.ca



Privacy Remains a Social Norm

“It is not that privacy has stopped being the norm; it’s that privacy is a dynamic that is a complex function based on an individual’s needs and choices – choices that must be respected and strongly protected if we are to maintain freedom and liberty in our society.”

— Commissioner Cavoukian,
Globe and Mail, March 15, 2010

Privacy *Remains* a Social Norm



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

Published on Monday, March 15, 2010
in the *The Globe and Mail*

There was a considerable amount of controversy recently when Mark Zuckerberg, co-founder and CEO of Facebook, the world’s most popular online social network, was misquoted as saying that “privacy is no longer a social norm.” What he actually said was: “People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.”

But few appear to recall his exact words – the take-away (erroneous though it may be) was that Mr. Zuckerberg no longer considered privacy to be a social norm (reflected in the many calls I received asking me to respond to that statement). While I would not presume to speak for Mr. Zuckerberg, his staff confirmed that his words were taken out of context.

What I emphatically submit is that there is little evidence to change our view that privacy remains a social norm. Privacy relates to freedom of choice and control in the sphere of one’s personal information – choices regarding what information

you wish to share and, perhaps more important, what you do not want shared with others. What has changed, however, is the means by which personal information is now readily exchanged, at the speed of light.

In the past, personal information was kept largely private because of limited personal exchange systems (i.e., live contact, telephone, snail mail). The technological means by which such information may now be shared has exploded – that is what has changed meteorically, not the collapse of privacy as a social norm. No doubt, technology may have an effect on a person’s ultimate choice of what personal information to share, but it should still be the individual who makes that choice – a decision conditional not only on technology but on other factors and needs in one’s life.

Let me speak for a moment as a psychologist (in my former life). The human condition requires connection: We are social animals who seek contact with each other. We also seek privacy: moments of solitude, intimacy, quiet, reserve and control – personal control. These interests have co-existed for centuries and must continue to do so, for the human condition requires both.

The fact that social media are growing exponentially does not negate that equation. What this explosion in technology does raise, however, is whether it is possible to preserve the notion of data protection in the online world. Can we continue to control and protect the personal information we share with others in social media, or are such media essentially becoming public spheres?

Let me point out the importance of taking a positive-sum (win/win) approach, instead of a zero-sum (win/lose) one, in tackling this. By adopting such a lens, one can easily see that people can have multiple interests that may co-exist.

Take the growth of online social networks and privacy. In this world of multi-tasking and limited attention span, a zero-sum approach in which the strengthening of one interest (connecting) leads to

Continued over page ...




Positive-Sum Model

*Change the paradigm
from a zero-sum to
a “positive-sum” model:
Create a win-win scenario,
not an either/or
involving unnecessary trade-offs
and false dichotomies*



Privacy by Design: The 7 Foundational Principles

1. *Proactive* not Reactive;
Preventative not Remedial
2. Privacy as the *Default*
3. Privacy *Embedded* into Design
4. Full Functionality:
Positive-Sum, not Zero-Sum
5. End-to-End Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy


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 that 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 asserts 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 understand that a more substantial approach is required – extending the use of PETs to taking a positive-sum, not a zero-sum, approach.

Privacy by Design now extends to a "Triology" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and 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 protection requirements tend to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* – ensuring privacy and personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the following principles:

1. **Proactive** not Reactive; **Preventative** not Remedial

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.



The Bottom Line

Privacy should be viewed as a
business issue, not a
compliance issue

**Think strategically and transform privacy
into a *competitive business advantage***



Ten Reasons for Building Consumer Trust

1. Avoiding damage to your company's and/or brand's reputation;
2. Avoiding penalization by any existing or pending laws;
3. Avoiding civil and class-action lawsuits;
4. Maintaining the balance of monitoring the activities of employees while not harming their morale and productivity;
5. Ensuring the continuation of valuable business relationships by ensuring your company measures up to the privacy standards adopted by strategic partners;



Ten Reasons for Building Consumer Trust (Cont'd)

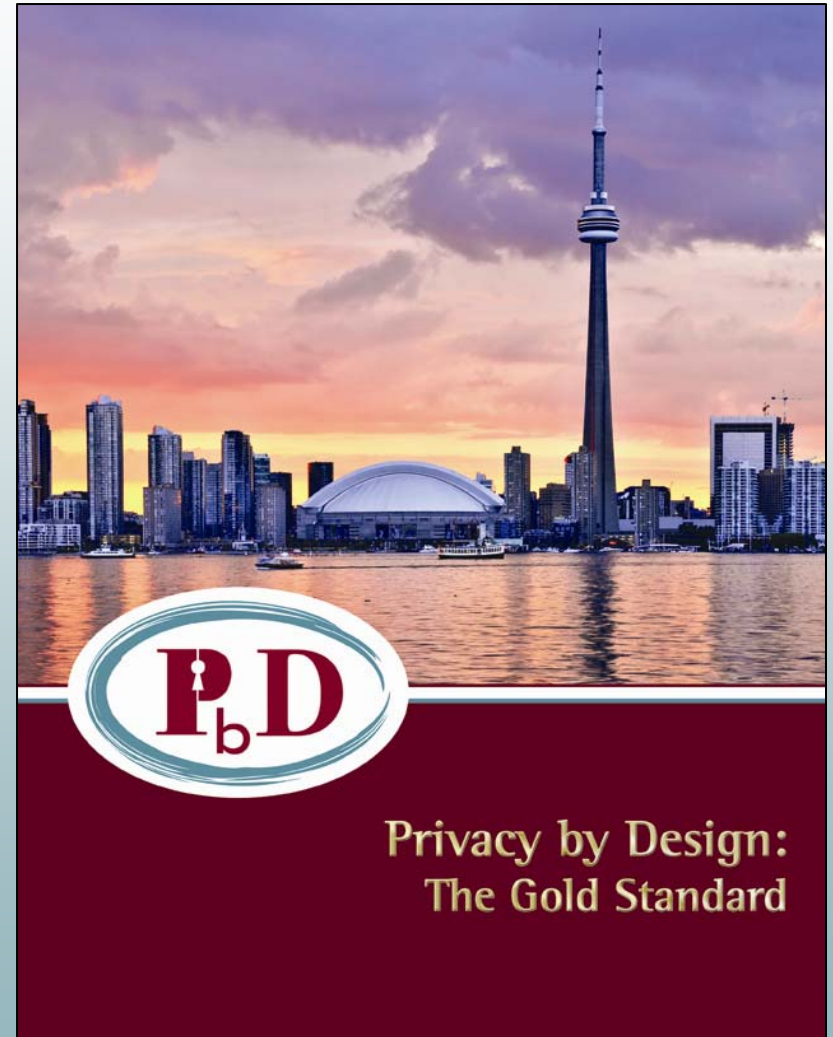
6. Being aware of the privacy laws and customs in other countries;
7. Gaining the trust and confidence of customers so that they will not provide you with false information;
8. Dealing with consumers who expect you to treat their personal information the same way that you would treat your own;
9. Repeat online customers are those who feel assured that shopping online is secure and their information is protected;
10. Gain and maintain an edge over your competitors through embracing more than just the minimum of laws, regulations and privacy best practices.

— Ann Cavoukian, Ph.D., Tyler Hamilton, *The Privacy Payoff: How Successful Businesses Build Consumer Trust*, McGraw-Hill Ryerson, 2002, pp. 13-14.



Privacy by Design: The Gold Standard

- Sold-out event in January 2010
- Celebrated practical successes that companies have achieved with *Privacy by Design*.

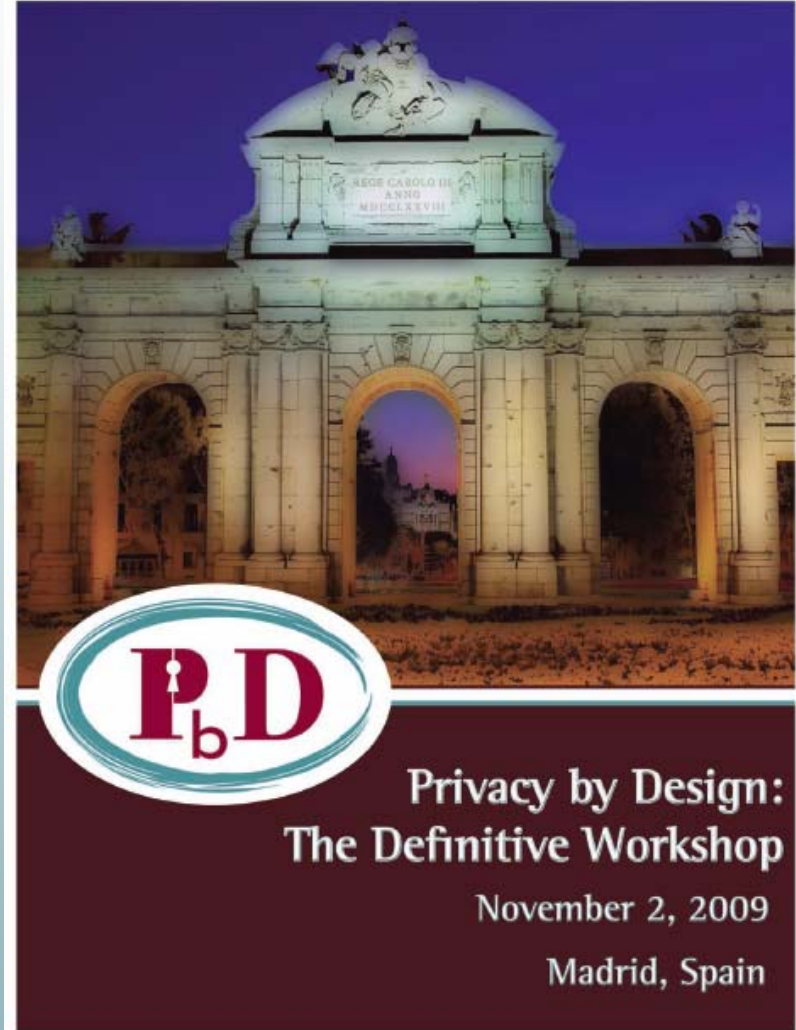


www.privacybydesign.ca/pbd2010.htm



Privacy by Design: The Definitive Workshop Madrid, Spain

- Sold out international event;
- First *Privacy by Design* event to an international audience;
- A call to action to advance the view that the future of privacy cannot be assured solely by relying on compliance with regulatory frameworks;
- Rather, we must strive to make privacy the default mode of operation.



www.privacybydesign.ca/madrid09.htm

BECOME A PRIVACY BY DESIGN AMBASSADOR



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



www.privacybydesign.ca



Questions You Should Have Answers to:

- Does your organization have a Data Map?
- Do you know all the points of entry for personally identifiable information (PII) into your organization?
- Do you know how customer data flows throughout your organization?
- Do you have a consent management system in place ... when you need to obtain additional consent from your customers?
- Is the data maintained securely, from end-to-end?



Conclusions

- Lead with *Privacy by Design* – embed privacy into the design specifications of information technologies, accountable business practices, operations and networked infrastructure;
- Change the paradigm from a zero-sum to a “positive-sum” model: Create a doubly-enabling win-win scenario;
- View privacy as a **business** issue, not a *compliance* issue – think strategically and transform privacy into a sustainable **competitive business advantage**;
- Privacy is a long-term investment, central to retaining existing customers – and essential to attracting new ones;
- Maintain your data securely, end-to-end; the potential for data breaches doesn’t end until the data are securely destroyed.



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