

“Privacy by Design”

*The Answer to Overcoming Negative Externalities
Arising from Poor Management of Personal Data*

Ann Cavoukian, Ph.D.

**Information and Privacy Commissioner
Ontario**

Trust Economics Workshop

London, England

June 23, 2009



Presentation Outline

- 1. Negative Externalities*
- 2. “Privacy by Design”*
- 3. Why Privacy is Good for Business*
- 4. Consumer Confidence and Trust*
- 5. Conclusions*



Negative Externalities



Privacy Vulnerabilities as a Negative Externality

- Violations of privacy can be viewed as an external cost or a “negative externality;”
- An external cost is essentially a cost produced by one entity, but borne by another.

— Ann Cavoukian, Ph.D. and Tyler Hamilton,
The Privacy Payoff: How Successful Businesses Build Customer Trust



How to Respond – Proactive or Reactive?

- How should those costs be handled?
 - **Proactive?** Privacy practices built-in up front – embedded;
 - **Reactive?** Regime of liability risk – litigation, after the fact;
- Proactive privacy practices are ultimately less expensive and more desirable; they also lead to a competitive advantage.

“The cost of a privacy PR blowout can range from tens of thousands to millions of dollars, depending on the company’s size and the visibility of its brand, and this does not include lost business and damage to reputation.”

— *Surviving the Privacy Revolution*,
Forrester Research.



Who Should be Responsible... Companies or Consumers?

- Placing the burden on companies to prevent privacy violations may increase their operating costs;
- The cost of placing the burden on consumers, however, would be prohibitive;
- In both cases, negative externality exists, regardless of who bears the costs;
- The burden should be placed where the cost is the least.

— Nobel Laureate, Ronald Coase,
Lowest cost strategy



Don't Blame the Victim

- Premise: violations of privacy are viewed as a negative externality;
- *Businesses however, not consumers, create privacy externalities through their misuse or lack of sufficient protection of their customers' personal information;*
- It would be far more costly for individuals to prevent or attempt to remedy the abuses of their personal information, if at all possible;
- **We place the responsibility for protecting customer's PII squarely upon business.**



www.privacybydesign.ca



“Privacy by Design”

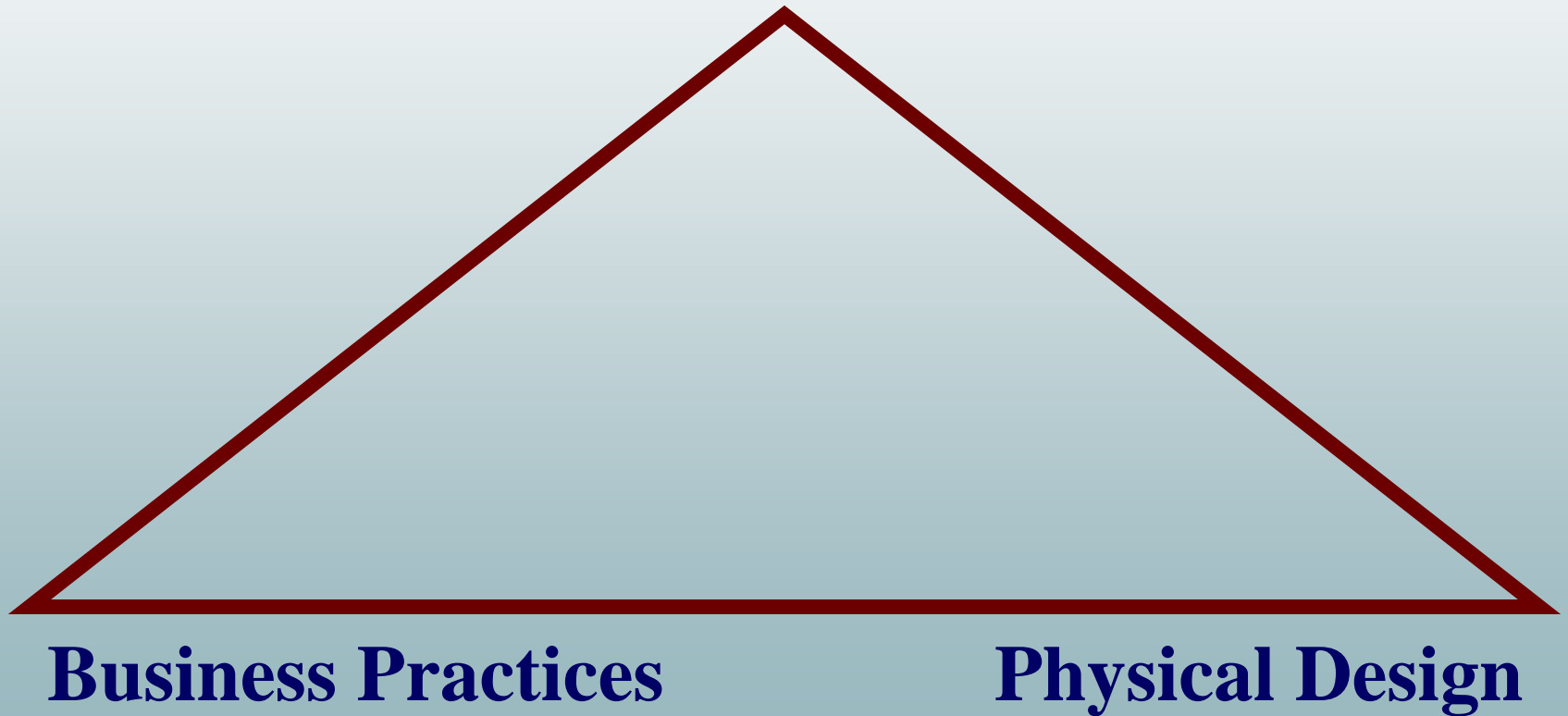
Privacy by Design: “Build It In”

- 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;
- “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 data;
- Privacy should always be the default – the default rules!



Privacy by Design: *The Trilogy of Applications*

Information Technology





Privacy by Design: *Focus for 2009*

- **Technology** – Building privacy directly into technology, at the earliest developmental stage;
- **Business Practices** – Incorporating privacy into competitive business strategies and operations;
- **Physical Design** – Introducing privacy into organizational and health care settings.



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, and unknown;
- Compliance alone is unsustainable as a model for ensuring the future of privacy; for that, we must turn to proactive measures, *Privacy by Design*: embed privacy proactively into the core of all that we do – make it the default.



*Why Privacy is Good
for Business*



The Bottom Line

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

Think of privacy as a sound business strategy



Costs of A Privacy Breach

- Legal liabilities, class action suits;
- Loss of client confidentiality and trust;
- Diminution of brand and reputation;
- Loss of customers, competitive edge;
- Penalties and fines levied;
- Costs of crisis management, damage control, review and retrofit of information systems, policies and procedures.



Consumer Confidence and Trust



Consumer Choice and Privacy

- There is a strong competitive advantage for businesses to invest in good data privacy and security practices;
- *“A significant portion of the population is becoming concerned about identity theft, and it is influencing their purchasing decisions.”*

— Rena Mears, Deloitte & Touche LLP,
*Survey Reports An Increase in ID Theft and Decrease in
Consumer Confidence, 2005.*



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)

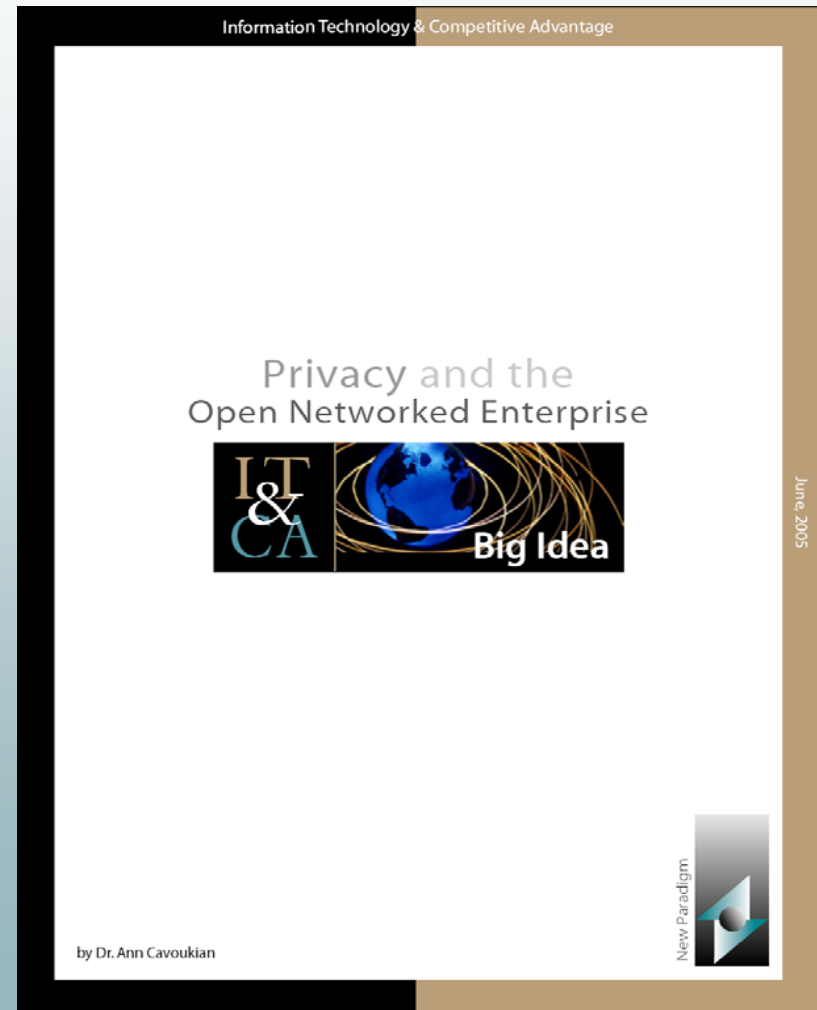
6. Being aware of the privacy laws and customs in other countries;
7. Gaining the trust and confidence of customers so that they will not provide you with false information;
8. Dealing with consumers who expect you to treat their personal information the same way that you would treat your own;
9. Repeat 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 and Security in the *Open Networked Enterprise*

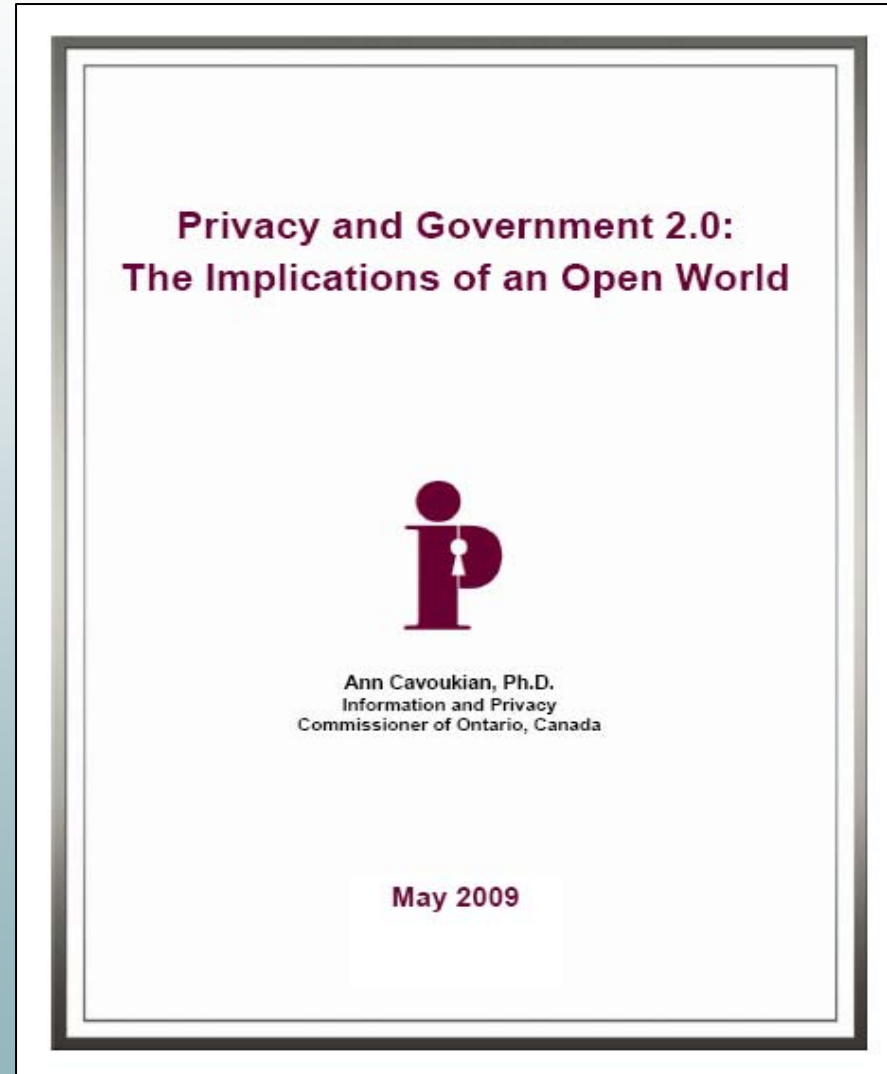
- A company adopting the **Open Networked Enterprise** model is confronted with fundamental questions relating to its treatment of personally identifiable information (PII):
 - With whom will it share its PII?
 - How will it manage that data internally?
 - How should it involve customers in managing their own PII?
 - What personal data will and should it receive from others?
 - Where should it set the limits of PII collection by new technologies?





Privacy and Government 2.0

- Privacy Defined
- Citizen Data Custodian
- A Positive-Sum Approach
- Data Accountability
- Data Minimization
- Data Security
- Data Access
- The Big Idea: Individual participation and control
- Data Co-Management



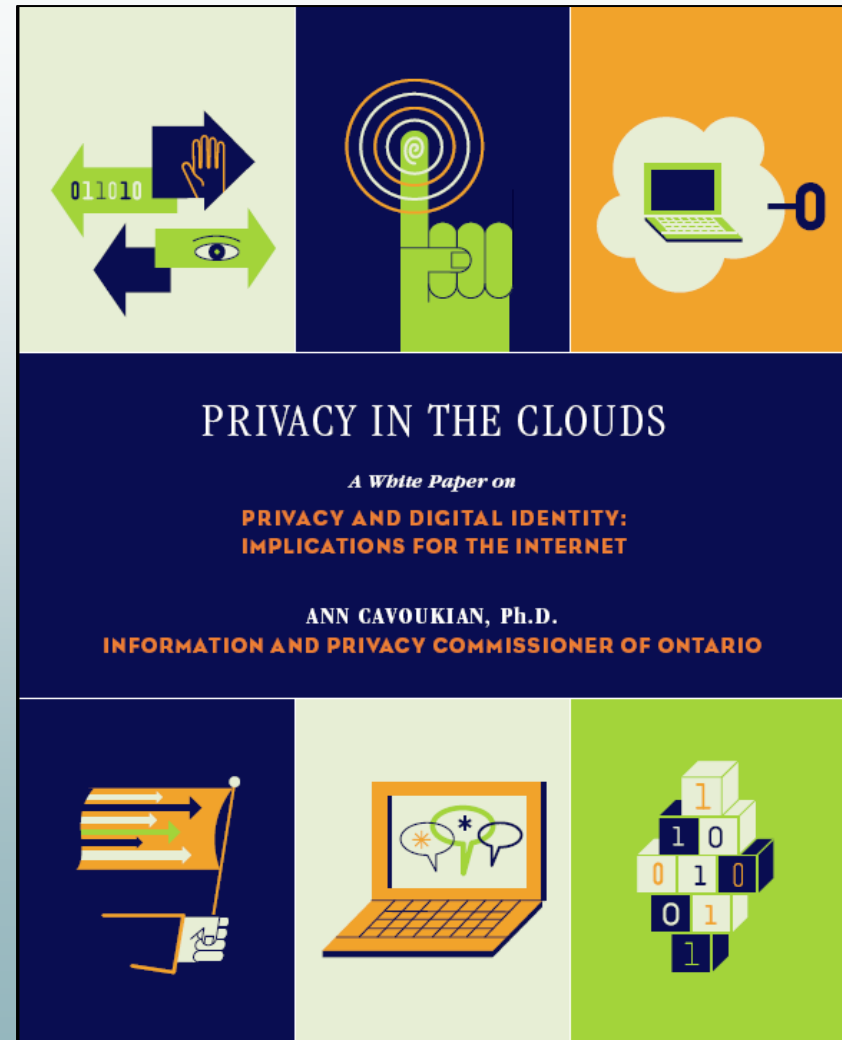


Privacy in the Clouds

(in the Web 2.0 World)

Cloud Building Blocks:

1. Open source and proprietary identity software based on open standards;
2. Federated Identity;
3. Multiple and partial identities;
4. Data-centred policies;
5. Audit tools.





Federated Privacy Impact Assessment (F-PIA)

Goals of an F-PIA:

- Provide an opportunity for members to develop and codify a Federation's privacy policies;
- Demonstrate that privacy policies, as defined by members of the Federation, will be met;
- Demonstrate that an appropriate technological architecture is in place to prevent, to the extent possible, accidental or malicious violations of privacy policies.





Evolutionary Perspective



Taking an Evolutionary Perspective

- In nature, when a species within an eco-system is exposed to an environmental stress (or a negative externality), stakeholders within the population will attempt different test-solutions to overcome the stress;
- Nature uses the mechanism of genetic mutations to evolve new behaviours in individuals within a species as test-solutions;
- Different test solutions are explored as an attempt to counteract environmental stress, allowing for continued survival of the species;
- The different test-solutions or genetic mutations are shaped by the constraints of the rules of nature.



Evolutionary Perspective (Cont'd)

- Likewise, if we want to solve the problem of a societal negative externality, the rules should be structured so that the maximum number of stakeholders, within an environment of cooperation and competition, attempt many different test-solutions, leading to the selection of most effective solution(s);
- In an evolutionary process – solutions will be dynamic and will evolve as things change;
- If the rules are structured so that personal data is viewed as a property right under law, using an evolutionary model, the solution to the negative externality of privacy infringement will be efficient, effective and equitable enforcement mechanisms.



Personal Data as Property

“We are not debating whether to move into a world where data are collected, used, and sold. We already live in that world. Given that we are here, how can we ensure that at least some control is granted to those whom these data are about? I advocate a property regime not because of the sanctity of property as an ideal, but because of its utility in serving a different but quite important ideal.”

— Lawrence Lessig,
Code and Other Laws in Cyberspace, 1999.

Conclusions

- Violations of privacy may be viewed as an external cost or negative externality, often created by business, therefore the cost of resolving the problem should be borne by business;
- “Privacy by Design” is a viable solution to the problem since it embeds privacy protection proactively into the design of IT and business practices – making privacy the default;
- Embedding privacy in a positive-sum manner enables both privacy *and* security to be delivered;
- Privacy is good for business and can lead to a sustainable competitive advantage;
- Consider taking an evolutionary perspective to the problem of privacy as a negative externality.

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

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca