Patience, Persistence, Faith …
The Long Road to Privacy by Design

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

IFIP SEC 2011 –
Future Challenges in Security and Privacy
Lucerne, Switzerland
June 9, 2011
Privacy = Freedom
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.*
Beware of Unintended Consequences

• Uncontrolled secondary uses of personal data, by chance – not by design;
• Data leakage (think Wi-Fi, geolocation data – think Apple);
• User-generated (but not controlled) data;
• Users getting permanently blacklisted from jobs;
• Users getting increases in insurance premiums – denial of claims – loss of benefits.
Privacy by Design: The Trilogy of Applications

- Information Technology
- Accountable Business Practices
- Physical Design & Networked Infrastructure
The Future of Privacy

Change the Paradigm to Positive-Sum, *NOT* Zero-Sum

And embed this directly into your code
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.

www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf
Reject Zero-Sum Models
Privacy vs. Security? No!
Why the Balance Metaphor Doesn’t Work

- Implies that privacy and security are always in conflict – not true;
- Suggests that a loss of privacy is *ipso facto* a gain in security – not true;
- Is balance always desirable? No, not if both interests may be achieved in unison – *positive-sum* is doubly-enabling.

* A false dichotomy with a thin analytical framework

Julian Sanchez
The Trouble with “Balance” Metaphors
Nothing to Hide: The False Tradeoff between Privacy and Security

“The debate between privacy and security has been framed incorrectly as a zero-sum game in which we are forced to choose between one value and the other. Why can't we have both?”

http://docs.law.gwu.edu/facweb/dsolove/
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”
Online Social Media
(Connecting)
AND
Privacy
(Control)
2011 – Year of the Engineer: Beware of Unintended Consequences
Privacy by ReDesign

PbRD
Invitation to the first *PbD* Privacy by ReDesign Workshop

33rd International Conference of Privacy and Data Protection Commissioners

November 1, 2011
Mexico City

[www.facebook.com/cfpconf](http://www.facebook.com/cfpconf)

Sponsored by American Express and Ernst & Young
Rethink, Redesign, and Revive: The 3 R’s of PbRD

- **Rethinking** invites organizations to look at their risk mitigation strategies, legacy systems, and processes – including information technologies, business practices, physical design, and infrastructure – to consider using alternative approaches that are more privacy-protective. This may include revisiting assumptions about how much personal information is necessary for the system to operate: can you manage with less PII?

- **Redesigning** represents the opportunity to enable or implement improvements in how the system functions from a privacy perspective, while also ensuring that it continues to achieve key business requirements in a positive-sum, win/win relationship;

- **Reviving** the system in a new, privacy-protective way is the ultimate goal – yielding new opportunities and avoiding the burden of costly data leakage.
**PbRD Next Steps: Future Direction**

- With *Privacy by Design* widely recognized as the new gold standard for the protection of personal information, there is a clear need for practical guidance as to how to accomplish its objectives and implement its principles:
  - American Express;
  - Ernst & Young;
  - ASU *Privacy by Design* Research Lab;
  - *PbD*-PIA;
- I look forward to the participation of industry leaders and experts in the development of tools and resources such as Risk Management Frameworks, IT Security tools, Project Management instruments and best practices.
Privacy by Design in Practice
Privacy by Design in Practice: A Few Practical Examples

• Biometric Encryption
• CCTV Surveillance Cameras
• Bering Media IP Geolocation
• Smart Grid Operations
• SmartData – the embodiment of PbD

For more examples of Privacy by Design in Practice visit: www.privacybydesign.ca
Privacy by Design Publications

Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept
November 2010

Redesigning IP Geolocation: Privacy by Design and Online Targeted Advertising
October 2010

Operationalizing Privacy by Design: The Ontario Smart Grid Case Study
February 2011

The Next Evolution in Data Protection: “SmartData”
Developed at IPSI, SmartData represents the future of privacy and the control of personal information online.

Intelligent “smart agents” introduced into IT systems virtually – thereby creating “SmartData,”
– a new approach to Artificial Intelligence that will revolutionize the field.

These and other Privacy by Design publications are available at www.privacybydesign.ca
New Developments

• Announcing a new partnership with a U.S. utility – San Diego Gas & Electric (a division of Sempra) to embed *Privacy by Design* into their Smart Meter dynamic pricing system;

• A new Smart Grid paper with Berlin Commissioner, Alexander Dix, to be released in September, 2011 – Stay tuned!

[www.privacybydesign.ca](http://www.privacybydesign.ca)
Privacy by Design, Accept No Imitations

Just because someone calls it PbD, doesn’t mean it is PbD
The Road Ahead

David vs. Goliath AND
Become a Privacy by Design Ambassador

1. Identify within your organization an emerging technology, business practice or infrastructure that intersects with personally identifiable information and work toward building the principles of Privacy by Design (PbD) into it.

2. Share your ideas in our “PbD Community Forum.” Go to www.privacybydesign.ca.

3. Spread the message! Whenever you find the opportunity, inform others about the advantages and benefits of Privacy by Design.

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

www.privacybydesign.ca
Conclusions

• Lead with *Privacy by Design* and *Privacy by ReDesign*;

• Change the paradigm from the dated “zero-sum” to the doubly-enabling “positive-sum;”

• Deliver *both* privacy AND security or any other functionality, in an empowering “win-win” paradigm – abandon false trade-offs;

• Reject imitations – strive for the Gold Standard;

• Embed privacy as a core functionality: the future of privacy (and freedom) may depend on it!
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