Privacy by Design: What’s Been Happening?

Ken Anderson
Assistant Commissioner (Privacy)
Ontario

Hong Kong
June 13, 2012

Key Definitions

- **Information privacy** refers to the right or ability of individuals to exercise control over the collection, use and disclosure by others of their personal information.

- **Personally-identifiable information** ("PII") can be biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational or reputational, and is the stuff that makes up our modern identity.

  Personal information must be managed responsibly. When it is not, accountability is undermined and confidence in our evolving information society is eroded.
What Privacy is Not

Privacy ≠ Security

Privacy and Security: The Difference

Security =

- Authentication
- Data Integrity
- Confidentiality
- Non-repudiation

Organizational control of information through information systems

Information Privacy = personal control
The Future of Privacy

We Need a Paradigm Shift

www.privacybydesign.ca
The Future of Privacy

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

Positive-Sum Paradigm

• A Zero-Sum Paradigm describes a concept or situation in which one party’s gains are balanced by another party’s losses – win/lose; either/or; enhancing security often comes at the expense of privacy – the more you have of one, the less you can have of the other;

• A Positive-Sum Paradigm, in contrast, describes a situation in which all participants may mutually gain together (win-win);

• To achieve a positive-sum model, privacy must be proactively built into the system so that privacy protections are engineered directly into the technology, right from the outset;

• As a result, the unnecessary collection and use of personal data is minimized while increasing data security and allowing greater individual control;

• By applying the positive-sum paradigm to new privacy-invasive technologies, we can achieve both security and privacy resulting in a “win-win” scenario.
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”

Privacy by Design:
The Trilogy of Applications

Information Technology
Accountable Business Practices
Physical Design & Networked Infrastructure
Privacy by Design: The 7 Foundational Principles

1. **Proactive** not Reactive;
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
Landmark Resolution Passed to Preserve the Future of 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

Privacy by Design:
Proactive in 25 Languages!

8. Estonian 17. Russian
9. Hebrew 18. Romanian
Privacy by Design Highlights: 2010/2012

Autumn 2010

- **October** – Regulators from around the world gathered in Jerusalem, unanimously passing a Resolution recognizing *Privacy by Design* as an essential component of privacy protection;

- **November** – European Commission released its report: *Comprehensive Approach on Personal Data Protection in the European Union*, pointing out the important role that *Privacy by Design* will play in ensuring data controllers meet their responsibilities;

Spring 2011

- **February** – Debate in the Dutch Senate on data protection and privacy, consistently referred to the need for *Privacy by Design*.

- **February** – GSMA published, *Mobile Privacy Principles*, with a framework for a *Privacy by Design* approach to mobile devices;

- **April** – European Union announced the *Privacy and Data Protection Impact Assessment Framework for RFID Applications* – a milestone agreement to put consumers’ privacy at the centre of smart tag technology (using a *Privacy by Design* solution) and to make sure privacy concerns are addressed before products go on the market;

- **April** – U.S. Senators John Kerry and John McCain cited *Privacy by Design* in their *Commercial Privacy Bill of Rights*;

Summer 2011

- **July** – Government of Qatar asked for comments regarding the inclusion of *Privacy by Design* as a key legislative principle;

- **July** – California Public Utility Commission recognized that, “…the Privacy by Design methodology offers a promising approach to ensuring that data practices promote privacy, not just in the FIP of data minimization, but in all aspects of privacy planning.;”

- **August** – The Czech Data Protection Authority endorsed EU privacy reforms, which will be characterized by *Privacy by Design*, responsibility and accountability;

- **August** – The New Zealand Law Commissioner, John Burrows, recommended that Privacy Commissioner, Marie Shroff, establish several expert panels which would advise on technical matters, including *Privacy by Design*;

- **August** – The Israeli Law, Information and Technology Authority (ILITA) made *Privacy by Design* one of its principal conditions for Google’s operation of its Street View cars in Israel.
Autumn 2011

• September – Ontario IPC joint paper with Berlin DPA on “Privacy by Design and Smart Metering: Minimize Personal Information to Maintain Privacy – Data Minimization at its Best;”

• October – San Diego Gas & Electric partnered with Ontario IPC to embed Privacy by Design into their Smart Meter Dynamic Pricing system.

January 2012

European Union Directive

• Privacy by Design and Privacy as the Default are specifically mentioned - Data controllers/processors must implement technical and organizational measures having regard to PbD;

• Independent Supervisory Authorities with investigative/order making powers may impose sanctions of up to 2% of a company’s annual revenue;

• Data Breach Notification- data controllers must notify Supervisory Authority within 24 hours of a data breach (where feasible) and individuals (without undue delay) where data is not encrypted.
The Year of the Engineer

Engaging Engineers
Privacy by Design and the Internet Engineering Task Force (IETF)

“The concept of Privacy by Design has gotten a lot of attention over the past few years and within the IETF we have tried to investigate how we can consider privacy in the design of protocols and architectures in a more systematic way ... in protocols and architectural designs.”

“We have started to shed more light on privacy in the IETF by organizing a privacy workshop to solicit input from the technically minded privacy community, to create an IETF privacy directorate, and to start the work on a number of documents to offer more guidance to engineers.”

— Privacy Considerations for Internet Protocols, Internet Engineering Task Force (IETF), www.ietf.org

Embedding Privacy at the Design Stage:
The Obvious Route

• Cost-effective
• Proactive
• User-centric
• It’s all about control – preserving personal control and freedom of choice over one’s data flows
1. **Rethink:** review existing risk mitigation strategies and systems, considering alternatives that will be more privacy protective;

2. **ReDesign:** develop and enable improvements in the system that will deliver original function and privacy in a doubly-enabling, positive-sum manner;

3. **Revive:** re-launch the newly improved, more privacy protective system.

http://privacybydesign.ca/content/uploads/2011/05/PbRD.pdf
• Identifying potential targets for Privacy by ReDesign;

• Practical framework for implementing Privacy by ReDesign;

• Laying the foundations for success;

• A road map towards proactive data protection.


---

Rise of the Privacy Economy

• A wave of startups are creating a new business model for the use of personal data;

• Rather than “cookies” tracking consumers' movements online, their alternative model would allow individuals to control their own data, and perhaps even profit by selling access to it;

• Some advocates predict the rise of a “privacy economy,” where Internet companies would provide services that allow people to discover what information exists about them online, to counter false information, and even allow people to control and share their personal information when it benefits them.

• Reputation.com

• Personal Data Ecosystem Consortium

• Consider Personal

• Singly
Respect Network
The World's First Personal Cloud Network

Drummond Reed
Co-Founder & Chairman
Respect Network Corporation
2010-04-04

Executive Summary

This presentation will explain how Respect Network Corporation is creating the world's first personal cloud network based on the award-winning Respect Trust Framework, and how this ethical business model for personal data will enable the leap from CRM to VRM (Vendor Relationship Management)
CRM (Customer Relationship Management) systems are used by vendors to manage their relationships with customers.

Social CRM tries to make CRM smarter by listening to what customers are sharing with their social networks.
VRM (Vendor Relationship Management) is the “inverse of CRM”: the idea that customers can have their own relationship management system that is a “peer” of the vendor's.

Although VRM is still an emerging segment, over 20 companies and open source projects already produce VRM software, services, and standards.
Such a trust framework already exists: the **Respect Trust Framework** was listed with OIX (Open Identity Exchange) and won the **Privacy Award** at the European Identity Conference in May 2011.
At a Crossroads: “Personhood” and Digital Identity in the Information Society

1. Data Protection in the IDM-Enabled Ubiquitous Information Environment
2. Data Protection and User Control
3. Market Demand for User Control
4. The Properties of Identity
5. The Properties of Identity and Data Protection
6. The Properties of Identity for Policy Makers and Software Developers
7. Current Conceptions of IDM
8. Decisions and Constraints

Identity and Privacy Crisis

Growing ID requirements pose privacy problems:

- **Fraud and security concerns** are inhibiting confidence, trust, and the growth of e-commerce, e-government
- **Fears of surveillance** and excessive collection, use and disclosure of identity information by others are also diminishing confidence and use
- **Lack of individual user empowerment and control** over one’s own personal data is diminishing confidence and use
- **Function creep, power asymmetries, discrimination, harm**

**Needed:** improved user control, data minimization techniques, architectures of privacy, stronger security, trusted devices and credible assurances.
Privacy-Embedded

Laws of Identity

Building User-Centric Privacy into an Identity Metasystem

- Emergence of Identity Metasystem a profound development – strategic time to ensure that privacy interests are built into the new global architecture of identity
- Supporters of 7 Laws of Identity and Identity Metasystem call this the “Identity Big Bang” to enable ubiquitous intelligent services and a true marketplace for portable identities
- Since we noticed many parallels between the 7 Laws of Identity and Fair Information Practices, the two sets of principles being fundamentally complementary, we decided to embed privacy directly into them
“Privacy-Embedded”
7 Laws of Identity

1. Personal Control and Consent:
   Technical identity systems must only reveal information identifying a user with the user’s consent.

2. Minimal Disclosure For Limited Use: Data Minimization
   The Identity Metasystem must disclose the least identifying information possible. This is the most stable, long-term solution. It is also the most privacy protective solution.

3. Justifiable Parties: “Need To Know” Access
   Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4. Directed Identity: Protection and Accountability
   A universal Identity Metasystem must be capable of supporting a range of identifiers with varying degrees of observability and privacy.

5. Pluralism of Operators and Technologies: Minimizing Surveillance
   The interoperability of different identity technologies and their providers must be enabled by a universal Identity Metasystem.

6. The Human Face: Understanding Is Key
   Users must figure prominently in any system, integrated through clear human-machine communications, offering strong protection against identity attacks.

7. Consistent Experience Across Contexts: Enhanced User Control
   The unifying Identity Metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.
Implications for Users

The 7 Privacy-Embedded “Laws” of Identity offer:

• Easier and more direct control over one’s personal information when online

• Embedded ability to minimize the amount of identifying data revealed online

• Embedded ability to minimize the linkage between different identities and online activities

• Embedded ability to detect fraudulent email messages and web sites (less spam, phishing, pharming, online fraud).
Privacy in the Clouds

• The 21st Century Privacy Challenge
• Creating a User-Centric Identity Management Infrastructure
  • Technology Building Blocks
• Call to Action

www.ipc.on.ca/images/Resources%5Cprivacyintheclouds.pdf
Creating A User-Centric Identity Management Infrastructure

- Adequate tools to manage personal information on all devices
- Infrastructure allowing unified user experience with all devices
- System with a clear framework of agreed upon rules
- “Sticky” policies that travel with the information and ensure proper use in accordance with policy
- Infrastructure that supports cross-system interaction as well as interoperation and delegation
- Open standards and community-driven interoperability
- Policies, mechanisms, and technologies that use only the amount of personal information necessary
- Diversity in identity management systems

Cloud Technology Building Blocks

- Open source and proprietary identity software based on open standards
- Federated identity
- Multiple and partial identities
- Data-centred policies
- Audit tools
Through the Clouds

Transforming Web 2.0 Technologies of Identity:

What you need to do …

Preserve and promote user privacy through:
• Enhanced user controls;
• Data minimization;
• Improved safeguards.

Develop user-centric identity technologies that are:
• Interoperable and easy to use;
• Based upon free and open standards;
• Trustworthy and accountable.

Privacy by Design Meets the Cloud

• There is a need and opportunity to engineer privacy, security and trust into new emergent Internet and web architectures:
  – Interoperable identity metasystems;
  – Cloud-based services, platforms and infrastructures;

http://www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf
Cloud Computing Architecture and Privacy

- Cloud Delivery Models
- Deployment Models
- Cloud Stack
- Data in the Cloud – Blurred Security Perimeter
- PbD Cloud Computing
- Protecting Privacy and Maintaining Access
- Protecting Privacy and Data Integrity

www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf
More Resources: Federated PIA

- Develop and codify a Federation’s privacy policies;
- Demonstrate that defined privacy policies 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.

More information can be found at [www.ipc.on.ca/images/Resources/F-PIA_2.pdf](http://www.ipc.on.ca/images/Resources/F-PIA_2.pdf).

Cloud Security Checklist

1. Discover How many projects you already have in the cloud;
2. Establish a cloud IT team and limit their administrative rights;
3. Don’t skip the evaluation stage;
4. Do a thorough risk assessment;
5. Begin classifying data and identifying what can be moved to the cloud and what should reside on-premise behind security layers;
6. Find a cloud-appropriate system for user authentication and access;
7. Scrutinize SLAs and ask:
   - What are the data privacy and retention policies?
   - Where is information stored?
   - If you terminate your service, how long will it take to get your data back and in what form will you get it?
   - What is the disaster recovery plan?


Privacy by Design Meets the Cloud: Outsourcing

• Cloud computing services present similar privacy challenges to outsourcing: Where is the personal data? Which jurisdiction and laws apply? Who is accountable for the data and its uses? Is there effective oversight?

Some things to consider:
• Conduct a Privacy Impact Assessment;
• Only use identifying information when necessary;
• Identify and minimize privacy and security risks;
• Use privacy enhancing technological tools;
• Exercise due diligence;
• Ensure transparency, notice, education & awareness;
• Develop a privacy breach management plan;
• Create and enforce contractual clauses.
Contractual Provisions to Consider when Outsourcing to Other Jurisdictions

- Require the service provider to agree not to use personal information to which it has access except as necessary in the course of providing services;
- Require the service provider to agree not to disclose personal information to which it has access in the course of providing services;
- Set out the administrative, technical and physical safeguards that must be employed by the service provider to ensure that records of personal information are retained, transferred and disposed of in a secure manner;
- Require the service provider to notify the organization, at the first reasonable opportunity, of any summons, order or similar requirement to compel production of the information issued outside Canada;
- Require the service provider to notify the organization, at the first reasonable opportunity, if the personal information is stolen, lost or accessed by unauthorized persons;
- Require the establishment of an oversight and monitoring program, including audits of the service provider’s compliance with the terms of the agreement; and
- Prohibit the service provider from permitting its employees or any person acting on its behalf from having access to the personal information unless the employee or person acting on its behalf agrees to comply with the restrictions set out in the agreement.
You can outsource services …

… but you can’t outsource accountability.

You always remain accountable.

Announcing:
“Privacy by Design in the Age of Big Data”

• 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.

www.privacybydesign.ca
Questions? Comments?

How to Contact Us

Ken Anderson
Office of the Information & Privacy Commissioner of Ontario
Toronto, Ontario, Canada
M4W 1A8
Phone: (416) 326-3333 / 1-800-387-0073
Web: www.ipc.on.ca
E-mail: ken.anderson@ipc.on.ca